Kaspersky Endpoint Detection and Response Expert (on-premises)

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky EDR Expert 8.3

Что нового

Исправленные ошибки

О Kaspersky EDR Expert

- Комплект поставки
- Аппаратные и программные требования
- Требования Kaspersky Deployment Toolkit
- Совместимые приложения и решения
- Архитектура Kaspersky EDR Expert
- Основные понятия
  - Сервер администрирования
  - Иерархия Серверов администрирования
  - Веб-сервер
  - Агент администрирования
  - Группы администрирования
  - Управляемое устройство
  - Нераспределенное устройство
  - Рабочее место администратора
  - Веб-плагин управления
  - Политики
  - Профили политик
  - Задачи
  - Область действия задачи
  - Взаимосвязь политики и локальных параметров приложения
  - Точка распространения
  - Шлюз соединения
  - Ядро
  - Хранилище
  - Коллектор
  - Коррелятор
  - События
  - Алерты
  - Инциденты
  - Ресурсы
  - Сервисы
  - Об уровне важности

О предоставлении данных

- О предоставлении данных
- Предоставление данных в Kaspersky Unified Monitoring and Analysis Platform
- Предоставление данных в Sandbox

Лицензирование

- О Лицензионном соглашении
- О лицензионном ключе

- О коде активации
- О файле ключа
- Активация Kaspersky EDR Expert
- Просмотр информации об используемых лицензионных ключах
- Отзыв согласия с Лицензионным соглашением
- Продление срока действия лицензии приложений "Лаборатории Касперского"
- Использование Kaspersky Marketplace для выбора бизнес-решений

Руководство по масштабированию

- Расчеты для компонентов Kaspersky EDR Expert
- Расчеты для развертывания Kaspersky EDR Expert на четырех узлах
- Расчеты для развертывания Kaspersky EDR Expert на шести узлах
- Расчеты для конфигурации кластера высокой доступности
- Расчеты для Sandbox

Развертывание Kaspersky EDR Expert

- Развертывание на одном узле с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS
- Развертывание на одном узле с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)
- Развертывание на нескольких узлах с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS
- Развертывание на нескольких узлах с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)
- Развертывание в отказоустойчивой конфигурации с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS
- Развертывание в отказоустойчивой конфигурации с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)
- Руководство по усилению защиты
  - Управление инфраструктурой Kaspersky EDR Expert
  - Безопасность соединения
  - Учетные записи и авторизация
  - Управление защитой Kaspersky EDR Expert
  - Управление защитой клиентских устройств
  - Передача событий в сторонние системы
  - Настройка защиты управляемых приложений
- Схемы развертывания
  - Схема развертывания на одном узле
  - Развертывание на нескольких узлах: схема профиля на четырех узлах
  - Развертывание на нескольких узлах: схема профиля на шести узлах
  - Развертывание с высокой доступностью: схема профиля на 14 узлах
  - Развертывание в нескольких ЦОД
- Порты, используемые Kaspersky EDR Expert
  - Изменение порта, используемого для подключения к серверу Консоли OSMP
  - Изменение порта, используемого Endpoint Agents для подключения к компоненту agentserver
- Подготовительные работы и развертывание
  - Развертывание на нескольких узлах: подготовка устройства администратора и целевых устройств
  - Развертывание на одном узле: подготовка устройства администратора и целевых устройств
  - Подготовка устройств к установке сервисов KUMA
  - Установка системы управления базами данных
  - Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky EDR Expert
  - Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes

Развертывание на нескольких узлах: параметры установки
Развертывание на одном узле: параметры установки
Подключение компонентов Endpoint Agent через прокси-узел
Мастер развертывания для Kaspersky EDR Expert
Установка Kaspersky EDR Expert
Настройка доступа в интернет целевых устройств
Синхронизация времени на машинах
Установка сервисов KUMA внутри кластера Kubernetes
Установка сервисов KUMA вне кластера Kubernetes
Развертывание нескольких кластеров Kubernetes и экземпляров Kaspersky EDR Expert
Установка и обновление Kaspersky EDR Expert в среде с физической изоляцией
Предварительная проверка готовности инфраструктуры для развертывания
Проверка целостности компонентов Kaspersky EDR Expert перед установкой
Вход в Kaspersky EDR Expert
Интеграция с Endpoint Agent
Подготовка и установка Sandbox
Подготовка ИТ-инфраструктуры к установке Sandbox
Подготовка виртуальной машины к установке Sandbox
Подготовка образа установочного диска
Установка Sandbox
Шаг 1. Ознакомление с Лицензионным соглашением и Политикой конфиденциальности
Шаг 2. Выбор диска для установки Sandbox
Шаг 3. Настройка минимальной длины пароля администратора Sandbox
Шаг 4. Создание учетной записи администратора Sandbox
Шаг 5. Настройка управляющего сетевого интерфейса
Шаг 6. Назначение имени устройства и добавление адресов DNS-серверов
Шаг 7. Настройка статического сетевого маршрута
Интеграция с Kaspersky Sandbox
Развертывание Kaspersky EDR Expert с высокой доступностью
Отказоустойчивая конфигурация Kaspersky EDR Expert
Восстановление отказавшего узла в кластере Kubernetes
Развертывание в нескольких ЦОД Kaspersky EDR Expert с высокой доступностью
Развертывание в нескольких ЦОД: подготовка устройства администратора и целевых устройств
Развертывание в нескольких ЦОД: параметры установки
Развертывание в нескольких ЦОД с перекрестным подключением с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS
Обслуживание Kaspersky EDR Expert
Обновление компонентов Kaspersky EDR Expert
Проверка целостности установленных компонентов Kaspersky EDR Expert
Изменение параметров Kaspersky EDR Expert без переустановки
Добавление и удаление управляющих и рабочих узлов кластера Kubernetes
Контроль версий конфигурационного файла
Удаление Kaspersky EDR Expert
Удаление компонентов Kaspersky EDR Expert вручную
Переустановка Kaspersky EDR Expert после неудачной установки
Переустановка компонентов Kaspersky EDR Expert
Остановка узлов кластера Kubernetes

Использование сертификатов для публичных служб Kaspersky EDR Expert
Расчет и изменение дискового пространства для хранения данных Сервера администрирования
Просмотр и изменение дискового пространства для Ядра KUMA и сервиса Метрики
Просмотр и изменение размера объектного хранилища
Увеличение размера хранилища наблюдаемости
Ротация сертификатов кластера Kubernetes
Ротация учетных данных для доступа к реестру
Ротация учетных данных СУБД и сертификатов
Добавление устройств для установки дополнительных сервисов KUMA
Замена устройства, использующего хранилище KUMA
Работа с Kaspersky EDR Expert, развернутым на виртуальных машинах
Настройка модели статусов инцидентов
Демонстрационное развертывание Kaspersky EDR Expert
Подготовка устройства администратора и целевых устройств
Указание параметров установки
Начало работы
Первоначальная настройка Kaspersky EDR Expert
Проверка настройки Kaspersky EDR Expert
Использование функций мониторинга, обнаружения и поиска угроз
Пример расследования инцидента с помощью Kaspersky EDR Expert
Обновление Kaspersky EDR Expert с версии 8.2 до версии 8.3
Перенос данных в Kaspersky EDR Expert
О переносе данных из Kaspersky Security Center Windows
Экспорт групповых объектов из Kaspersky Security Center Windows
Импорт файла экспорта в Kaspersky EDR Expert
Переключение управляемых устройств под управление Kaspersky EDR Expert
О переносе данных из KEDR 7.1
Настройка компонента SIEM и работа с ним
Службы KUMA
Инструменты сервисов
Получение идентификатора сервиса
Остановка, запуск и проверка статуса сервиса
Перезапуск службы
Удаление службы
Просмотр таблицы активных запросов
Окно Разделы
Поиск связанных событий
Наборы ресурсов для сервисов
Создание хранилища
Структура кластера ClickHouse
Параметры узлов кластера ClickHouse
Холодное хранение событий
Удаление дисков холодного хранения
Отключение, архивирование и подключение партиций
Создание набора ресурсов для хранилища
Создание службы хранилища в OSMP
Установка хранилища в сетевой инфраструктуре OSMP

Резервное копирование, восстановление и импорт партиций
Резервное копирование партиций по расписанию
Резервное копирование партиций вручную
Импорт партиций из стороннего экземпляра OSMP
Восстановление партиций из резервной копии
Создание коллектора
Запуск мастера установки коллектора
Шаг 1. Подключение источников событий
Шаг 2. Транспорт
Шаг 3. Парсинг событий
Шаг 4. Фильтрация событий
Шаг 5. Агрегация событий
Шаг 6. Обогащение события
Шаг 7. Маршрутизация
Шаг 8. Проверка параметров
Установка коллектора в сетевой инфраструктуре KUMA
Проверка правильности установки коллектора
Обеспечение бесперебойной работы коллекторов
Управление потоком событий с помощью rsyslog
Управление потоком событий с помощью nginx
Предустановленные коллекторы
Создание коррелятора
Запуск мастера установки коррелятора
Шаг 1. Общие параметры коррелятора
Шаг 2. Глобальные переменные
Шаг 3. Корреляция
Шаг 4. Обогащение
Шаг 5. Действие по реагированию
Шаг 6. Маршрутизация
Шаг 7. Проверка параметров
Установка коррелятора в сетевой инфраструктуре OSMP
Проверка правильности установки коррелятора
Создание коррелятора correlator-ng
Настройка коррелятора correlator-ng
Поддерживаемые типы данных correlator-ng
Селекторы правил корреляции и выражения
Атрибуты правила корреляции standard
Функции обработки данных в корреляторе-ng
Настройка источников событий
Настройка получения событий Auditd
Установка коллектора KUMA для получения событий Auditd
Настройка сервера источника событий
Настройка получения событий KATA/EDR
Настройка передачи событий KATA/EDR в KUMA
Создание коллектора KUMA для получения событий KATA/EDR
Установка коллектора KUMA для получения событий KATA/EDR

Интеграция с другими решениями
Интеграция с Kaspersky Security Center
Настройка интервала обновления данных для активов Kaspersky Security Center
Расписание импорта активов Kaspersky Security Center
Ручной импорт активов Kaspersky Security Center
Просмотр иерархии Серверов администрирования Kaspersky Security Center
Импорт событий из базы Kaspersky Security Center
Интеграция с Kaspersky CyberTrace
Интеграция поиска по индикаторам CyberTrace
Настройка CyberTrace для приема и обработки запросов
Создание правил обогащения событий
Интеграция интерфейса CyberTrace
Подключение по протоколу LDAP
Включение и выключение LDAP-интеграции
Добавление тенанта в список тенантов для интеграции с LDAP-сервером
Создание подключения к LDAP-серверу
Создание копии подключения к LDAP-серверу
Изменение подключения к LDAP-серверу
Изменение периода обновления данных
Изменение срока хранения данных
Запуск задач на обновление данных об учетных записях
Удаление подключения к LDAP-серверу
Интеграция с Kaspersky Industrial CyberSecurity for Networks
Настройка интеграции в KICS for Networks
Настройка интеграции в KUMA
Включение и выключение интеграции с KICS for Networks
Изменение периода обновления данных
Особенности импорта информации об активах из KICS for Networks
Изменение статуса актива KICS for Networks
Интеграция с Neurodat SIEM IM
Kaspersky Automated Security Awareness Platform
Создание токена в KASAP и получение ссылки для API-запросов
Настройка интеграции в KUMA
Просмотр данных о пользователях KASAP и изменение учебных групп
Отправка уведомлений в Telegram
Создание и настройка бота в Telegram
Создание скрипта для отправки уведомлений
Настройка отправки уведомлений в KUMA
Интеграция с UserGate
Настройка интеграции в UserGate
Подготовка скрипта для интеграции с UserGate
Настройка правила реагирования для интеграции с UserGate
Интеграция с Kaspersky Web Traffic Security
Настройка интеграции в KWTS
Подготовка скрипта для интеграции с KWTS
Настройка правила реагирования для интеграции с KWTS

Интеграция с Kaspersky Secure Mail Gateway
Настройка интеграции в KSMG
Подготовка скрипта для интеграции с KSMG
Импорт информации об активах из RedCheck
Настройка получения событий Sendmail
Настройка журналирования Sendmail
Настройка передачи событий Sendmail
Настройка интеграции с внешней SIEM-системой
Управление KUMA
Настройка параметров Ядра KUMA
Прокси-серверы
Подключение к SMTP-серверу
Работа с задачами Kaspersky Security Center
О создании задач KUMA в Kaspersky Security Center
Запуск задач Kaspersky Security Center вручную
Автоматический запуск задач Kaspersky Security Center
Проверка статуса задач Kaspersky Security Center
Журналы KUMA
Уведомления KUMA
Изменение профиля пользователя KUMA
Работа с тенантами
Управление сертификатами
Скачивание сертификатов
Изменение самоподписанного сертификата веб-интерфейса
Перевыпуск внутренних CA-сертификатов
Перевыпуск сертификата для отдельного сервиса
Работа с геоданными
Формат геоданных
Конвертация геоданных из MaxMind и IP2Location
Импорт и экспорт геоданных
Сопоставление геоданных по умолчанию
Работа с базой знаний
Просмотр сведений о пакете
Просмотр сведений о ресурсе
Установка и обновление пакетов и ресурсов
Ресурсы KUMA
Операции с ресурсами
Создание, переименование, перемещение и удаление папок с ресурсами
Создание, дублирование, перемещение, редактирование и удаление ресурсов
Привязка ресурсов к службам
Обновление ресурсов
Настройка пользовательского источника с использованием Kaspersky Update Utility
Экспорт ресурсов
Импорт ресурсов
Управление тегами

Точки назначения
- Точка назначения, тип internal
- Тип nats-jetstream
- Тип tcp
- Тип udp
- Тип http
- Тип diode
- Тип kafka
- Тип файла
- Тип storage
- Тип correlator
- Предустановленные точки назначения

Нормализаторы
- Параметры парсинга событий
- Расширенная схема события
  - Добавление полей расширенной схемы событий
  - Изменение полей расширенной схемы событий
  - Импорт и экспорт полей расширенной схемы событий
  - Удаление полей расширенной схемы событий
  - Использование полей расширенной схемы событий в нормализаторах
- Генерация регулярных выражений с помощью KIRA
- Обогащение в нормализаторе
- Условия передачи данных в дополнительный нормализатор
- Поддерживаемые источники событий

Правила агрегации

Правила обогащения

Правила корреляции
- Правила корреляции типа standard
- Правила корреляции типа simple
- Правила корреляции типа operational
- Переменные в корреляторах
  - Локальные переменные в группирующих и уникальных полях
  - Локальные переменные в селекторе
  - Локальные переменные в обогащении событий
  - Локальные переменные в обогащении активных листов
  - Свойства переменных
  - Требования к переменным
  - Функции переменных
  - Объявление переменных
- Предустановленные правила корреляции
- Добавление временного списка исключений для корреляционного правила
- Конвертер правил Sigma
  - Подготовка правил Sigma
  - Примеры поддерживаемых конвертаций правил Sigma
- Покрытие матрицы MITRE ATT&CK

Фильтры

Активные листы
- Просмотр таблицы активных листов
- Добавление активного листа
- Просмотр параметров активного листа
- Изменение параметров активного листа
- Дублирование параметров активного листа
- Удаление активного листа
- Просмотр записей в активном листе
- Поиск записей в активном листе
- Добавление записи в активный лист
- Дублирование записей в активном листе
- Изменение записи в активном листе
- Удаление записей в активном листе
- Импорт данных в активный лист
- Экспорт данных из активного листа
- Предустановленные активные листы

Словари

Правила реагирования
- Правила реагирования для Kaspersky Security Center
- Правила реагирования для пользовательского скрипта
- Правила реагирования для KICS for Networks
- Правила реагирования для Kaspersky Endpoint Detection and Response
- Правила реагирования через Active Directory

Правила сбора и анализа данных

Виртуальный Сервер администрирования

Коннекторы
- Просмотр параметров коннектора
- Добавление коннектора
- Параметры коннекторов
  - Тип kata/edr

Секреты

Контекстные таблицы
- Просмотр списка контекстных таблиц
- Добавление контекстной таблицы
- Просмотр параметров контекстной таблицы
- Изменение параметров контекстной таблицы
- Дублирование параметров контекстной таблицы
- Удаление контекстной таблицы
- Просмотр записей контекстной таблицы
- Поиск записей в контекстной таблице
- Добавление записи в контекстную таблицу
- Изменение записи в контекстной таблице
- Удаление записи из контекстной таблицы
- Импорт данных в контекстную таблицу
- Экспорт данных из контекстной таблицы

Построение иерархии экземпляров OSMP
Подключение дочернего экземпляра к родительскому экземпляру
Назначение подчиненного Сервера администрирования в иерархии экземпляров OSMP
Отключение дочернего экземпляра от родительского экземпляра
Распределение правил корреляции в иерархии
Распространение глобальной конфигурации коррелятора вместе с глобальными правилами корреляции
Распространение глобальных правил корреляции для локального использования
Дублировать унаследованные правила корреляции для локального использования
Просмотр ресурсов и сервисов, созданных в дочерних экземплярах OSMP
Поведение папок при распределении ресурсов в иерархии
Объединение экземпляров OSMP в иерархию
Восстановление иерархии экземпляров после ротации сертификатов
Интерфейс Консоли OSMP
Изменение языка интерфейса Консоли OSMP
Изменение домашней страницы OSMP Console
Добавление и удаление закладок
Новая навигация в KEDR
Обнаружение угроз
Работа с алертами
Об алертах
Модель данных алерта
Просмотр таблицы алертов
Просмотр деталей алерта
Назначение алертов аналитикам
Изменение статуса алерта
Создание алертов вручную
Связь алертов с инцидентами
Удаление связи алертов с инцидентами
Связывание событий с алертами
Удаление связи событий с алертами
Поиск событий, связанных с импортированным алертом IOA
Работа с алертами на графе расследования
Добавление IOA-правила в исключения
Управление правилами агрегации
Создание правил агрегации
Изменение правил агрегации
Копирование правил агрегации в другой тенант
Удаление правил агрегации
Работа с инцидентами
Об инцидентах
Модель данных инцидента
Создание инцидентов
Создание дочерних инцидентов
Просмотр таблицы инцидентов
Просмотр сведений об инциденте
Назначение инцидентов аналитикам
Изменение статуса инцидента

Изменение приоритета инцидента
Объединение инцидентов
Экспорт инцидентов в файл
Создание инцидентов Managed Detection and Response из EDR-инцидентов
Правила сегментации
Копирование правил сегментации в другой тенант
Управление Service Level Agreement (SLA)
Создание Service Level Agreement (SLA)
Удаление Service Level Agreement (SLA)
Работа с типами инцидентов
Просмотр таблицы типов инцидентов
Создание типов инцидентов
Изменение типов инцидентов
Удаление типов инцидентов
Управление типами рабочих процессов
Просмотр таблицы рабочих процессов инцидентов
Предустановленные рабочие процессы инцидентов
Рабочий процесс по ГОСТ
Создание рабочих процессов инцидентов
Изменение рабочих процессов и статусов инцидентов
Удаление рабочих процессов инцидентов
Управление трудозатратами инцидентов
Добавление трудозатрат инцидентов
Изменения трудозатрат инцидентов
Удаление трудозатрат инцидентов
Создание и экспорт отчетов об инцидентах
Настройка периода хранения алертов и инцидентов
Просмотр информации об активе
Исследование и реагирование с помощью удаленного терминала
Управление подключениями удаленных терминалов
Выполнение действий по реагированию с помощью удаленного терминала
Поиск угроз
Модель данных событий
Process
File Create
File Modify
File Rename
File Read
File Delete
File Attributes Modify
File Creation Time Modify
File Hardlink Created
File Symlink Created
Module
Registry Create
Registry Delete
Registry Modify

Registry Rename
Registry Query
Registry Save
Connection
Port Listen
AMSI Scan
Process Console Input
Driver
Process Interpreted File Run
DNS
Pipe Create
Pipe Connect
LDAP
WMI Activity
WMI Consumer Register
Code Injection
Process Access
Threat Detect
Threat Detect Processing Result
Linux Event Log
Windows Event Log
Blocked Document
Applock
Process Terminated
Device
File System Mount
File System Unmount
Bits Job Create
Bits Job Complete
Bits Job Start
Bits Job Stop
Bits Job Add File
Bits Job Error
Service Create
Service Modify
Service Delete
Scheduled Task Create
Scheduled Task Modify
Scheduled Task Delete
File Owner Change
File ACL Change
Registry Owner Change
Registry ACL Change
Executable Memory Mapped
Agent Start
Agent Stop
Agent Install

Agent Uninstall
Agent Action
System Startup
System Shutdown
Connection Close
Работа с событиями
Гранулярный доступ к событиям
Просмотр таблицы событий
Поиск и фильтрация событий
Создание SQL-запросов вручную
Формирование SQL-запроса с помощью конструктора
Формирование SQL-запроса с помощью SQL-функций KUMA
Использование набора функций enrich в SQL-запросах
Использование набора функций lookup в SQL-запросах
Просмотр сведений о событии
Сохранение и выбор конфигурации фильтра событий
Фильтрация событий по периоду
Экспорт событий
Просмотр событий аудита и настройка уведомлений
События аудита
Ретроспективное сканирование
Получение статистики таблицы событий
Реагирование на угрозы
Действия по реагированию
Прерывание процессов
Перемещение файлов на карантин
Выполнение действий по реагированию Добавить правило запрета и Удалить правило запрета
Управление службами
Получение файлов для дальнейшего анализа
Получение файла
Получение ключа реестра
Получение метафайлов NTFS
Получение данных для расследования
Получение образа диска
Получение дампа памяти
Получение дампа памяти процесса
Получение файлов из карантина
Проверка устройств на наличие угроз
Сканирование YARA
IOC-проверка
Удаление файла
Реагирование с помощью Active Directory
Включение и отключение сетевой изоляции
Запуск приложения
Просмотр истории реагирования из деталей алерта или инцидента
Работа с файлами, полученными в результате действий по реагированию

Работа с таблицей правил запрета
Создание правила запрета
Импорт правил запрета
Работа с таблицей IOC-правил
Работа с таблицей YARA-правил
Плейбуки
Действия по реагированию, доступные в плейбуках
Просмотр таблицы плейбуков
Создание плейбуков
Настройка шагов выполнения плейбука в визуальном редакторе
Изменение плейбуков
Настройка плейбуков
Просмотр свойств плейбука
Прерывание работы плейбуков
Удаление плейбуков
Управление версиями плейбука
Сравнение версий плейбука
Восстановление версий плейбука
Запуск плейбука в тестовом режиме
Запуск плейбуков и действий по реагированию
Запуск плейбуков вручную
Запуск плейбуков для объектов, указанных пользователями
Запуск плейбуков в режиме Обучение
Настройка ручного подтверждения действий по реагированию
Подтверждение плейбуков или действий по реагированию
Обогащение из плейбуков
Просмотр истории реагирования
Предустановленные плейбуки
[KL] P001 "Creation of executable files by office applications"
[KL] P002 "Windows Event Log was cleared"
[KL] P003 "Suspicious child process from wmiprvse.exe"
[KL] P004 "Sandbox Medium Detect"
[KL] P005 "Sandbox High Detect"
[KL] "Playbook for checking external IP addresses"
[KL] "Playbook for isolating a device where an infected file is detected"
[KL] "Playbook for isolating a device where an infected file is detected"
[KL][EDR] "Delete malicious files transferred to the host from alert"
[KL][EDR] "Delete malicious files transferred to the host from incident"
[KL][EDR] "Isolate host when Discovery activity is detected from alert"
[KL][EDR] "Isolate host when Discovery activity is detected from incident"
[KL][EDR] "Isolate host when Exfiltration activity is detected"
[KL][EDR] "Isolate host when reverse shell activity is detected from alert"
[KL][EDR] "Isolate host when reverse shell activity is detected from incident"
[KL][EDR] "Mitigate malicious activity from email attachments from alert"
[KL][EDR] "Mitigate malicious activity from email attachments from incident"
[KL][EDR] "Mitigate memory dumping activity from alert"
[KL][EDR] "Mitigate memory dumping activity from incident"

Триггер плейбука
Алгоритм плейбука
Параметры плейбука
Параметры шага выполнения
Loop
Parallel
Decision
UpdateData
Параметры ResponseFunction
AI-сервисы
AI рейтинг и AI-статус активов
Установка сервиса AI-рейтинг и AI-статус активов
Перевыпуск сертификата AI-сервиса
Параметры настройки сервиса AI-рейтинг и AI-статус активов
Настройка интеграции с KIRA с использованием поставщика LLM
Анализ алертов и инцидентов с помощью KIRA
Настройка интеграции с KIRA с использованием KSN
Выполнение анализа с помощью KIRA
Возможные ошибки задачи Проанализировать с помощью KIRA
Создание поисковых запросов на естественном языке с помощью KIRA
Создание поисковых запросов на естественном языке и их преобразование в SQL-запросы с помощью KIRA
Возможные ошибки при создании запроса на естественном языке
Настройка обнаружения атак DLL Hijacking
Настройка обнаружения взломанных учетных записей
Управление объектами в хранилищах
Загрузка файлов для проверки
Проверка файлов в разделе Файлы вручную
Просмотр статуса и результатов проверки
Загрузка файлов из разделов Карантин и Файлы резервного хранилища
Восстановление файлов из карантина
Удаление файлов из карантина
Об удалении объектов из разделов Карантин, Файлы резервного хранилища или Активные угрозы
Управление активами
Интеграция с другими решениями
Интеграция с Kaspersky Managed Detection and Response
Интеграция с Kaspersky Security Network
Настройка доступа к KSN
Включение и отключение участия в KSN и KPSN
Настройка подключения к локальной репутационной базе KPSN
Настройка отправки обнаруженных объектов в список запрещенных KPSN
Просмотр Положения о Kaspersky Security Network
Интеграция с Kaspersky Threat Intelligence Portal
Взаимодействие с НКЦКИ
Настройка интеграции с НКЦКИ
Просмотр таблицы инцидентов НКЦКИ
Просмотр сведений об инциденте НКЦКИ
Создание инцидента НКЦКИ

Передача инцидентов в НКЦКИ
Допустимые категории и типы инцидентов НКЦКИ
Статусы инцидента НКЦКИ
Управление Sandbox
Первоначальная настройка Sandbox
Настройка обновления баз для Sandbox
Сетевые интерфейсы Sandbox
Настройка параметров DNS
Настройка управляющего сетевого интерфейса
Настройка доступа в интернет для обрабатываемых объектов
Добавление статического сетевого маршрута
Изменение пароля учетной записи администратора Sandbox
Политики аутентификации в Sandbox
Завершение неактивных сеансов в Sandbox
Информирование о неуспешных попытках аутентификации на Sandbox
Подготовка виртуальных машин к работе
Загрузка образов в Хранилище
Импорт шаблона
Создание пользовательского шаблона виртуальной машины
Настройка операционной системы и программного обеспечения
Создание виртуальной машины
Установка виртуальной машины
Загрузка отладочных символов
Настройка OSMP для использования технологий обнаружения
Обновление антивирусных баз Sandbox и Anti-Malware Engine
Создание списка паролей для архивов, защищенных паролем
Выбор операционных систем для проверки объектов в Sandbox
Создание пользовательских правил Sandbox
Настройка отправки файлов от Endpoint Agent в Sandbox
Об индикаторах компрометации, IOC-файлах и IOC-правилах
Настройка IOC-проверки по расписанию
Импорт IOC-правил
Импорт YARA-правил
Работа с Open Single Management Platform
Настройка Сервера администрирования
Настройка адреса подключения Сервера администрирования
Настройка параметров подключения OSMP Console к Серверу администрирования
Настройка параметров доступа к интернету
Сертификаты для работы с Open Single Management Platform
О сертификатах Open Single Management Platform
Требования к пользовательским сертификатам, используемым в Open Single Management Platform
Перевыпуск сертификата для Консоли OSMP
Замена сертификата для OSMP Console
Преобразование сертификата из формата PFX в формат PEM
Сценарий: задание пользовательского сертификата Сервера администрирования
Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert
Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

Иерархия Серверов администрирования
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Просмотр списка подчиненных Серверов администрирования
Управление виртуальными Серверами администрирования
Создание виртуального Сервера администрирования
Включение и выключение виртуального Сервера администрирования
Назначение администратора виртуального Сервера администрирования
Смена Сервера администрирования для клиентских устройств
Удаление виртуального Сервера администрирования
Настройка журнала событий подключения к Серверу администрирования
Настройка количества событий в хранилище событий
Изменение учетных данных СУБД
Удаление иерархии Серверов администрирования
Доступ к общедоступным DNS-серверам
Настройка интерфейса
Шифрование подключения TLS
Обнаружение устройств в сети
Сценарий: обнаружение сетевых устройств
Опрос сети Windows
Опрос IP-диапазонов
Опрос контроллеров домена
Настройка контроллеров домена Samba
Использование динамического режима VDI на клиентских устройствах
Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования
Перемещение в группу администрирования устройств, являющихся частью VDI
Управление клиентскими устройствами
Параметры управляемого устройства
Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk
Создание групп администрирования
Правила перемещения устройств
Создание правил перемещения устройств
Копирование правил перемещения устройств
Условия для правила перемещения устройств
Добавление устройств в состав группы администрирования вручную
Перемещение устройств или кластеров в состав группы администрирования вручную
О кластерах и массивах серверов
Свойства кластеров или массивов серверов
Настройка точек распространения и шлюзов соединений
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
Расчет количества и конфигурации точек распространения
Автоматическое назначение точек распространения
Назначение точек распространения вручную
Изменение списка точек распространения для группы администрирования
Включение push-сервера
О статусах устройства
Настройка переключения статусов устройств

Выборки устройств
Просмотр списка устройств из выборки устройств
Создание выборки устройств
Настройка выборки устройств
Экспорт списка устройств из выборки устройств
Удаление устройств из групп администрирования в выборке
Теги устройств
Теги устройств
Создание тегов устройств
Изменение тегов устройств
Удаление тегов устройств
Просмотр устройств, которым назначен тег
Просмотр тегов, назначенных устройству
Назначение тегов устройству вручную
Удаление назначенного тега с устройства
Просмотр правил автоматического назначения тегов устройствам
Изменение правил автоматического назначения тегов устройствам
Создание правил автоматического назначения тегов устройствам
Выполнение правил автоматического назначения тегов устройствам
Удаление правил автоматического назначения тегов с устройств
Шифрование и защита данных
Просмотр списка зашифрованных жестких дисков
Просмотр списка событий шифрования
Формирование и просмотр отчетов о шифровании
Предоставление доступа к зашифрованному жесткому диску в автономном режиме
Передача ключей шифрования между Серверами администрирования
Смена Сервера администрирования для клиентских устройств
Просмотр и настройка действий, когда устройство неактивно
Удаленный доступ к управляемым устройствам
Удаленный доступ с Linux-устройства с Консолью OSMP к управляемому Linux-устройству
Удаленный доступ с Linux-устройства с Консолью OSMP к управляемому Windows-устройству
Удаленный доступ с Windows-устройства с Консолью OSMP к управляемому Linux-устройству
Удаленный доступ с Windows-устройства с Консолью OSMP к управляемому Windows-устройству
Управление активами
Добавление категории активов
Настройка таблицы активов
Поиск активов
Экспорт данных об активах
Просмотр информации об активе
Добавление активов
Добавление информации об активах в OSMP
Импорт информации об активах из Kaspersky Security Center
Импорт информации об активах из KICS for Networks
Примеры сравнения полей активов при импорте
Назначение активу категории
Изменение параметров активов
Архивирование активов

Удаление активов
Удаление категории активов
Массовое удаление активов
Обновление приложений сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center
Перемещение активов в выбранную группу администрирования
Аудит активов
Настройка аудита активов
Хранение и поиск событий аудита активов
Включение и выключение аудита активов
Настраиваемые поля активов
Активы критической информационной инфраструктуры
Развертывание приложений "Лаборатории Касперского"
Сценарий: развертывание приложений "Лаборатории Касперского"
Мастер развертывания защиты
Шаг 1. Запуск мастера развертывания защиты
Шаг 2. Выбор инсталляционного пакета
Шаг 3. Выбор способа распространения файла ключа или кода активации
Шаг 4. Выбор версии Агента администрирования
Шаг 5. Выбор устройств
Шаг 6. Задание параметров задачи удаленной установки
Шаг 7. Управление перезагрузкой
Шаг 8. Удаление несовместимых приложений перед установкой
Шаг 9. Перемещение устройств в папку Управляемые устройства
Шаг 10. Выбор учетных записей для доступа к устройствам
Шаг 11. Запуск установки
Добавление плагина управления для приложений "Лаборатории Касперского"
Удаление веб-плагина управления
Просмотр списка компонентов, интегрированных в Open Single Management Platform
Просмотр названий, параметров и пользовательских действий компонентов Kaspersky EDR Expert
Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"
Создание инсталляционных пакетов из файла
Создание автономного инсталляционного пакета
Изменение ограничения на размер пользовательского инсталляционного пакета
Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)
Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования
Просмотр списка автономных инсталляционных пакетов
Распространение инсталляционных пакетов на подчиненные Серверы администрирования
Подготовка устройства с операционной системой Linux к установке Агента администрирования
Установка приложений с помощью задачи удаленной установки
Удаленная установка приложений
Установка приложений на подчиненные Серверы администрирования
Указание параметров удаленной установки на устройствах под управлением Unix
Запуск и остановка приложений "Лаборатории Касперского"
Замещение приложений безопасности сторонних производителей
Удаленная деинсталляция приложений или обновлений программного обеспечения

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования
Подготовка устройства под управлением Windows к удаленной установке
Настройка приложений "Лаборатории Касперского"
Сценарий: настройка защиты сети
Подходы к управлению безопасностью, ориентированные на устройства и на пользователей
Настройка и распространение политик: подход, ориентированный на устройства
Настройка и распространение политик: подход, ориентированный на пользователя
О переключении Агента администрирования на другой Сервер администрирования
Создание профиля соединения для автономных пользователей
Политики и профили политик
О политиках и профилях политик
Блокировка (замок) и заблокированные параметры
Наследование политик и профилей политик
Иерархия политик
Профили политик в иерархии политик
Как параметры реализованы на управляемом устройстве
Управление политиками
Просмотр списка политик
Создание политики
Общие параметры политик
Изменение политики
Включение и выключение параметра наследования политики
Копирование политики
Перемещение политики
Экспорт политики
Импорт политики
Принудительная синхронизация
Просмотр диаграммы состояния применения политики
Автоматическая активация политики по событию "Вирусная атака"
Удаление политики
Управление профилями политик
Просмотр профилей политики
Изменение приоритета профиля политики
Создание профиля политики
Копирование профиля политики
Создание правила активации профиля политики
Удаление профиля политики
Экспорт и импорт профиля политики
Параметры политики Агента администрирования
Использование Агента администрирования для Windows, Linux и macOS: сравнение
Сравнение параметров Агента администрирования по операционным системам
Настройка параметров защиты управляемых приложений
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
О KSN
Настройка доступа к KSN
Включение и выключение использования KSN

Просмотр принятого Положения о KSN
Принятие обновленного Положения о KSN
Проверка, работает ли точка распространения как прокси-сервер KSN
Просмотр статистики работы прокси-сервера KSN
Управление задачами защиты конечных точек
О задачах
Область задачи
Создание задачи
Запуск задачи вручную
Запуск задачи для выбранных устройств
Просмотр списка задач
Общие параметры задач
Экспорт задачи
Импорт задачи
Запуск мастера изменения паролей задач
Шаг 1. Выбор учетных данных
Шаг 2. Выбор выполняемого действия
Шаг 3. Просмотр результатов
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security
Управление задачами обнаружения и реагирования
Просмотр таблицы задач
Просмотр результатов выполнения задачи
Повторный запуск задачи
Теги приложений
Создание тегов приложений
Изменение тегов приложений
Назначение тегов приложениям
Снятие назначенных тегов с приложений
Удаление тегов приложений
Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в OSMP Console
Обновление баз и приложений "Лаборатории Касперского"
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"
Создание задачи Загрузка обновлений в хранилище Сервера администрирования
Просмотр полученных обновлений
Проверка полученных обновлений
Создание задачи загрузки обновлений в хранилища точек распространения
Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования
Одобрение и отклонение обновлений программного обеспечения
Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows
Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"
Включение функции загрузки файлов различий
Загрузка обновлений точками распространения
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Удаленная диагностика клиентских устройств
Открытие окна удаленной диагностики
Включение и выключение трассировки для приложений
Загрузка файла трассировки приложения
Удаление файлов трассировки
Загрузка параметров приложений
Загрузка системной информации с клиентского устройства
Загрузка журналов событий
Запуск, остановка и перезапуск приложения
Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux
Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах
Использование компонента Контроль приложений для управления исполняемыми файлами
Режимы и категории компонента Контроль приложений
Получение и просмотр списка приложений, установленных на клиентских устройствах
Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Создание категории приложений, в которую входят исполняемые файлы из выбранных папок
Просмотр списка категорий приложений
Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows
Добавление исполняемых файлов, связанных с событием, в категорию приложения
Параметры задачи поиска уязвимостей и требуемых обновлений
О лицензии
Справочное руководство OpenAPI
Управление приложениями Endpoint Agent
Мониторинг, отчеты и аудит
Сценарий: мониторинг и отчеты
О типах мониторинга и отчетах
Срабатывание правил в режиме Интеллектуального обучения
Просмотр и подтверждение обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
Добавление исключений в правила Адаптивного контроля аномалий
Панель мониторинга и виджеты
Использование панели мониторинга
Виджеты администрирования и защиты
Добавление виджета на информационную панель
Удаление виджета с информационной панели
Перемещение виджета на информационной панели
Изменение размера или внешнего вида виджета
Изменение параметров виджета
Веб-виджеты обнаружения и реагирования
Основные принципы работы с виджетами
Особенности отображения данных в виджетах
Создание виджета
Изменение виджета

Удаление виджета
Параметры виджетов
Виджет События
Виджет Активные листы
Виджет Контекстные таблицы
Пользовательский виджет Активы
Другие виджеты
Фильтрация данных на виджетах
Фильтрация данных на одном виджете
Фильтрация данных на нескольких виджетах
Переход в связанную панель мониторинга
Отображение названий тенантов в виджетах типа Активный лист
Информационная панель Обнаружение и реагирование
Создание макета панели мониторинга
Выбор макета панели мониторинга
Выбор макета панели мониторинга по умолчанию
Изменение макета панели мониторинга
Удаление макета панели мониторинга
Включение и отключение режима ТВ
Преднастроенные макеты панели мониторинга
О режиме Просмотра только панели мониторинга
Настройка режима Просмотра только панели мониторинга
Отчеты администрирования и защиты
Использование отчетов
Шаблон отчета
Создание шаблона отчета
Просмотр и изменение свойств шаблона отчета
Удаление шаблонов отчетов
Универсальность шаблона отчетов
Экспорт отчета в файл
Генерация и просмотр отчета
Создание задачи рассылки отчета
Отчеты обнаружения и реагирования
Шаблон отчета
Создание шаблона отчета
Настройка расписания отчетов
Изменение шаблона отчета
Копирование шаблона отчета
Удаление шаблона отчета
Экспорт и импорт шаблона отчета
Универсальность шаблона отчетов
Сформированные отчеты
Просмотр отчетов
Создание отчетов
Сохранение отчетов
Обновление отчетов
Удаление отчетов

- События и выборки событий
  - О событиях в Kaspersky EDR Expert
  - События компонентов Kaspersky EDR Expert
    - Структура данных описания типа события
    - События Сервера администрирования
      - Критические события Сервера администрирования
      - События отказа функционирования Сервера администрирования
      - События предупреждения Сервера администрирования
      - Информационные события Сервера администрирования
    - События Агента администрирования
      - События предупреждения Агента администрирования
      - Информационные события Агента администрирования
  - Использование выборок событий
  - Создание выборки событий
  - Изменение выборки событий
  - Просмотр списка выборки событий
  - Экспорт выборки событий
  - Импорт выборки событий
  - Просмотр информации о событии
  - Экспорт событий в файл
  - Просмотр истории объекта из события
  - Удаление событий
  - Удаление выборок событий
  - Настройка срока хранения события
  - Блокировка частых событий
    - О блокировке частых событий
    - Управление блокировкой частых событий
    - Отмена блокировки частых событий
  - Обработка и хранение событий на Сервере администрирования
- Ретроскан
- Уведомления и статусы устройств
  - Использование уведомлений
  - Просмотр экранных уведомлений
  - О статусах устройства
  - Настройка переключения статусов устройств
  - Настройка параметров доставки уведомлений
  - Проверка распространения уведомлений
  - Параметры и переменные среды для описания события
- Мониторинг источников событий
  - Состояние источников
    - Список источников событий
  - Политики мониторинга
- Объявления "Лаборатории Касперского"
  - Об объявлениях "Лаборатории Касперского"
  - Выключение объявлений "Лаборатории Касперского"

Cloud Discovery
Включение функции Cloud Discovery с помощью виджета
Добавление виджета Cloud Discovery в панель мониторинга
Просмотр информации об использовании облачных сервисов
Уровень риска облачных сервисов
Блокировка доступа к нежелательным облачным сервисам
Экспорт событий в SIEM-системы
Настройка экспорта событий в SIEM-системы
Предварительные условия
Об экспорте событий
О настройке экспорта событий в SIEM-системе
Выбор событий для экспорта в SIEM-системы в формате Syslog
О выборе событий для экспорта в SIEM-систему в формате syslog
Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog
Выбор общих событий для экспорта в формате Syslog
Об экспорте событий в формате Syslog
Об экспорте событий в форматах CEF и LEEF
Конвертация событий в формат CEF или LEEF
Настройка Kaspersky EDR Expert для экспорта событий в SIEM-систему
Мониторинг изменений политики и профилей политик
Экспорт событий напрямую из базы данных
Выполнение SQL-запроса с помощью утилиты klsql2
Пример SQL-запроса, созданного с помощью утилиты klsql2
Просмотр имени базы данных Kaspersky EDR Expert
Просмотр результатов экспорта
Отправка событий из коллектора OSMP в коллектор внешней SIEM-системы
Работа с ревизиями объектов
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Откат изменений объекта к предыдущей ревизии
Операции по диагностике компонентов Kaspersky EDR Expert
Получение файлов журнала компонентов Kaspersky EDR Expert
Просмотр метрик OSMP
Мониторинг состояний компонентов Kaspersky EDR Expert
Просмотр метрик Longhorn
Просмотр панелей мониторинга и метрик EDR
Просмотр панели мониторинга Node Exporter Full
Настройка уведомлений по электронной почте о событиях работоспособности кластера Kubernetes
Управление адресами получателей уведомлений по электронной почте о событиях работоспособности кластера Kubernetes
Добавление параметров подключения к SMTP-серверу в конфигурационный файл без переустановки Kaspersky EDR Expert
Мониторинг сервисов
Просмотр метрик KUMA
Условия срабатывания алертов по метрикам KUMA
Хранение диагностической информации о компонентах Kaspersky EDR Expert

Получение файлов трассировки
Запись событий запусков пользовательских действий
Управление пользователями и ролями пользователей
Об учетных записях пользователей
О ролях пользователей
Настройка прав доступа к функциям приложения. Управление доступом на основе ролей
Права доступа к функциям приложения
Предопределенные роли пользователей
Назначение прав доступа к набору объектов
Назначение прав пользователям или группам пользователей
Добавление учетной записи внутреннего пользователя
Создание группы безопасности
Изменение учетной записи внутреннего пользователя
Настройка доменной аутентификации Kerberos
Изменение статуса пользователя
Изменение группы безопасности
Назначение роли пользователю или группе безопасности
Добавление учетных записей пользователей во внутреннюю группу безопасности
Назначение пользователя владельцем устройства
Настройка двухфакторной аутентификации
О двухфакторной аутентификации учетной записи
Настройка секретного ключа двухфакторной аутентификации при входе в Консоль OSMP
Разрешение для настройки двухфакторной аутентификации пользователям
Сброс и удаление секретного ключа двухфакторной аутентификации
Исключение учетных записей из двухфакторной аутентификации
Изменение имени издателя кода безопасности
Количество попыток ввода пароля
Настройка времени жизни пользовательских сеансов единого входа и токенов аутентификации
Удаление пользователей или групп безопасности
Изменение пароля учетной записи пользователя
Добавление пользовательского баннера на страницу входа
Создание роли пользователя
Изменение роли пользователя
Изменение области для роли пользователя
Удаление роли пользователя
Связь профилей политики с ролями
Мультитенантность
О привязке Серверов администрирования к тенантам
Настройка интеграции с Open Single Management Platform
Просмотр и изменение тенантов
Добавление тенантов
Назначение ролей пользователям и группам тенанта
Удаление тенантов
Настройка параметров отправки уведомлений по электронной почте
Создание шаблона уведомления
Изменение и удаление шаблона уведомления
Настройка автоматической ротации файлов в разделе Файлы

Резервное копирование и восстановление данных Kaspersky EDR Expert
Настройка хранилища для резервной копии Kaspersky EDR Expert
Настройка и управление расписанием резервного копирования
Создание резервной копии данных Kaspersky EDR Expert вручную
Просмотр резервных копий данных Kaspersky EDR Expert
Восстановление данных Kaspersky EDR Expert из резервной копии
Kaspersky EDR Expert API
Создание токена
Авторизация запросов API
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Известные проблемы и ограничения
Глоссарий
Bootstrap
EPP-программа
IOA-правило
IOC-файл
Kaspersky Deployment Toolkit
Lightweight Nagent (LWNGT)
Network Location Awareness (NLA)
Агент
Агент администрирования
Актив
Алгоритм плейбука
Алерт
Граф расследования
Действия по реагированию
Дистрибутив
Инцидент
Кластер Kubernetes
Коллектор
Контекст
Конфигурационный файл
Коррелятор
Маршрутизатор событий
Мультитенантность
Наблюдаемые объекты
Нормализованное событие
Плейбук
Получить данные для расследования
Пользовательские действия
Правила сегментации
Правило корреляции
Реестр
Сервисы KUMA
Событие

- Тенант
- Транспортный архив
- Узел
- Устройство администратора
- Файл инвентаря KUMA
- Хранилище
- Целевые устройства
- Цепочка развития угрозы

Информация о стороннем коде

Уведомления о товарных знаках

The MITRE Corporation Terms of Use

Справка Kaspersky EDR Expert 8.3

Новые функции

- Что нового в Kaspersky EDR Expert

Ключевые функции

- Управление алертами и инцидентами безопасности
- Инструменты Поиска угроз
- Граф расследования
- Предопределенные и пользовательские плейбуки
- Ручное реагирование на обнаруженные угрозы
- Панель мониторинга и виджеты

Совместимость и аппаратные и программные требования

- Аппаратные и программные требования
- Совместимые приложения и решения
- Интеграция с другими решениями

Начало работы

- Развертывание Kaspersky EDR Expert
- Начало работы
- Использование функций мониторинга, обнаружения и поиска угроз
- Пример расследования инцидента с помощью Kaspersky EDR Expert

Работа с Open Single Management Platform

- Установка приложений безопасности "Лаборатории Касперского" на устройства в корпоративной сети
- Удаленный запуск задач поиска вредоносного ПО и обновления
- Управление политиками безопасности управляемых приложений

Что нового

В Kaspersky EDR Expert (on-premises) 8.3 (далее также Kaspersky EDR Expert) реализован ряд новых возможностей и улучшений:

- В окне с деталями алерта и инцидента в разделе **Наблюдаемые объекты** вы можете выполнить поиск в таблице наблюдаемых объектов по данным из столбца **Значение**.
- При добавлении или удалении алерта из инцидента в статусе **Новый** приоритет инцидента автоматически пересчитывается. Значение приоритета заполняется значением **Уровень важности инцидента**.
- Обновлены контракты с НКЦКИ.
- Доступны новые предустановленные плейбуки:
  - [KL][EDR] Mitigate malicious activity from email attachments from alert.
  - [KL][EDR] Mitigate malicious activity from email attachments from incident.
  - [KL][EDR]Mitigate memory dumping activity from alert.
  - [KL][EDR]Mitigate memory dumping activity from incident.
  - [KL][EDR] Isolate host when Discovery activity is detected from alert.
  - [KL][EDR] Isolate host when Discovery activity is detected from incident.
  - [KL][EDR] Isolate host when Exfiltration activity is detected.
  - [KL][EDR] Delete malicious files transferred to the host from alert.
  - [KL][EDR] Delete malicious files transferred to the host from incident.
  - [KL][EDR] Isolate host when reverse shell activity is detected from alert.
  - [KL][EDR] Isolate host when reverse shell activity is detected from incident.

Исправленные ошибки

В таблицах ниже перечислены ошибки, обнаруженные в предыдущих версиях Kaspersky EDR Expert и исправленные в текущей версии.

Список ошибок, исправленных в Kaspersky EDR Expert 8.3

Первая затронутая версия	Идентификатор проблемы	Описание проблемы
8.2	10563365	Добавлен коннектор **HTTP Streaming**.
8.2	10562746	При использовании решения по лицензии Kaspersky EDR Expert эндпоинт `/xdr/api/v3/kuma/assets` корректно возвращает все ресурсы, доступные текущему пользователю в Консоли OSMP.
8.1	6962370	При переносе данных с подчиненного Сервера администрирования Kaspersky Security Center Windows на главный Сервер администрирования Kaspersky EDR Expert мастер переноса данных не завершает шаг **Импорт данных**. Эта проблема возникает, если вы создаете глобальную задачу на подчиненном Сервере администрирования (например, задачу *Удаленная установка приложения*) и выбираете только значение **Сервер администрирования Kaspersky Security Center** для параметра **Управляемые приложения для экспорта** в мастере переноса данных.
8.2	10419559	При изменении условия `EventType` в ходе изменения правила исключения возникает ошибка *У вас уже есть правило с таким названием*.
8.2	10593484	После обновления до версии 8.2 ресурсы, отчеты и виджеты панели мониторинга корректно отображаются при использовании решения по лицензии Kaspersky EDR Expert.
8.2	10624497, 10634081	Резервные копии данных Kaspersky EDR Expert создаются корректно.
8.2	10469536	В разделе **Лицензии** корректно отображается ограничение на количество учетных записей.
8.1	10687160	Домашняя страница, выбранная пользователем, отображается корректно.
8.1	10676575	Исправлена ошибка *Неправильная настройка Kaspersky Next XDR Expert* при входе в консоль OSMP.
7.0	8690777	Запуск стороннего пользовательского скрипта с использованием плейбука поддерживается только на устройствах Linux.
8.1	10664457	Исправлена проблема повышенного потребления памяти при открытии карточки инцидента.
8.1	10663896	При изменении политики добавленные ранее устройства не отображаются в списке устройств.
8.2	10644701	При изменении политики добавленное правило сохраняется корректно.
8.1	10536807	Изменение настроек политики для Kaspersky Endpoint Security для Windows 14.1 происходит корректно.
8.2	10442087	Создание политики Kaspersky Endpoint Security для Windows в OSMP происходит корректно.
8.0	—	Перенос данных телеметрии с Kaspersky EDR Expert версии 7.1 на версию 8.0 без лицензии Kaspersky Symphony XDR производится корректно.
8.1	—	Кнопка **Live shell** без лицензии Kaspersky Symphony XDR отображается корректно.

Список ошибок, исправленных в Kaspersky EDR Expert 8.2

Первая затронутая версия	Идентификатор проблемы	Описание проблемы
8.1	10386561	Невозможно было отменить запрос на подключение тенанта.
8.1	10317761	Загрузка дерева процессов при использовании Поиска угроз была отложена.
8.1	10063913	Запросы к конечной точке `/api/v1/alerts` вернули HTTP `500 Internal Server Error`.
8.1	10011047	Для тенантов, созданных до обновления до версии 8.1, функция IOC-проверки по расписанию могла отображаться в интерфейсе как включенная, в то время как IOC-проверка по расписанию была выключена.
8.1	6919635	После создания нового тенанта алерты, связанные с ним, отправлялись на сервер, но не отображались в таблице алертов.
8.1	6962370	При переносе данных с подчиненного Сервера администрирования Kaspersky Security Center Windows на главный Сервер администрирования Kaspersky EDR Expert **Мастер переноса данных** не завершал шаг Импорт данных. Эта проблема возникала, если вы создавали глобальную задачу на подчиненном Сервере администрирования (например, задачу **Удаленная деинсталляция приложения**) и выбирали только значение Сервера администрирования Kaspersky Security Center для параметра **Управляемые приложения для экспорта** в мастере переноса данных.
8.1	8690777	Запуск стороннего пользовательского скрипта с использованием плейбука поддерживался только на устройствах Linux.
8.0	9365692	Были добавлены инструкции для подключения к Консоли OSMP защищаемого хоста, если он заблокирован антивирусом.
8.1	9959974	В окне свойств устройства на вкладке **События** находился параметр **Выбрать все** для удаления событий. С помощью этого параметра можно было удалить все события из базы данных Сервера администрирования, включая события других устройств и события Сервера администрирования.
8.1	6646913	В графе расследования перестановка узлов выполнялась неправильно.
8.1	6704698	Плейбуки, содержащие действия по реагированию с помощью Kaspersky Endpoint Security для Windows, отображались как доступные в списке плейбуков, даже если веб-плагин Kaspersky Endpoint Security для Windows не был установлен в Kaspersky EDR Expert.
8.1	6810101	В окне свойств Сервера администрирования содержались параметры для мобильных устройств, однако Kaspersky EDR Expert не поддерживал управление мобильными устройствами.
8.1	7367358	После добавления или удаления тенантов в разделе **Тенанты** (**Параметры** → **Тенанты**) изменения в списке тенантов не синхронизировались с фильтром тенантов в разделе **Поиск угроз**.

Список ошибок, исправленных в Kaspersky EDR Expert 8.1

Первая затронутая версия	Идентификатор проблемы	Описание проблемы
8.0	9577853	Исправлена ошибка, из-за которой нельзя было менять имя хоста для Agentserver и Updater в конфигурационном файле.
8.0	9652285 9680467 9666950	Исправлена ошибка, из-за которой после переноса данных из Kaspersky Security Center Windows в Kaspersky EDR Expert 8.0 политики становились недоступными.

О Kaspersky EDR Expert

Kaspersky EDR Expert – это надежное решение для кибербезопасности, которое защищает вашу корпоративную ИТ-инфраструктуру от сложных киберугроз, в том числе тех, которые не могут быть обнаружены EPP-программами, установленными на корпоративных активах. Решение обеспечивает полную видимость, корреляцию и автоматизацию, используя широкий спектр инструментов реагирования и источников данных, включая активы конечных точек, данные сети и облачного окружения. Чтобы эффективно защитить вашу ИТ-инфраструктуру, Kaspersky EDR Expert анализирует данные из этих источников для выявления угроз, создает алерты о потенциальных инцидентах и предоставляет инструменты для реагирования на них. Kaspersky EDR Expert обладает расширенными аналитическими возможностями и богатым опытом в области безопасности.

Это решение обеспечивает единый процесс обнаружения и реагирования с помощью интегрированных компонентов и целостных сценариев в едином интерфейсе для повышения эффективности специалистов по безопасности.

Средства обнаружения включают:

- Инструменты поиска угроз для автоматического поиска угроз и уязвимостей путем анализа событий.
- Расширенное обнаружение угроз и корреляция: корреляция в режиме реального времени событий, основанных на готовых правилах корреляции для различных сценариев с сопоставлением с матрицей MITRE ATT&CK, возможность создавать правила и настраивать существующие, ретроспективное сканирование для обнаружения уязвимостей нулевого дня.
- Граф расследования для визуализации и облегчения расследования инцидента и определения первопричин алерта.
- Использование Kaspersky Threat Intelligence Portal для получения последней подробной информации об угрозах, касающейся веб-адресов, доменов, IP-адресов, хешей файлов, статистических и поведенческих данных, и данных WHOIS и данных DNS.

Инструменты действий по реагированию включают:

- Действия по реагированию, выполняемые вручную: изоляция активов, запуск команд, создание правил запрета, запуск задач на активе, обогащение репутации Kaspersky Threat Intelligence Portal и обучающие задания для пользователей.
- Плейбуки как предустановленные, так и созданные пользователем, для автоматизации типичных действий по реагированию.

Kaspersky EDR Expert также использует компонент Open Single Management Platform для управления активами и централизованного выполнения задач по администрированию и обслуживанию:

- Развертывание приложений "Лаборатории Касперского" на активах в корпоративной сети.
- Удаленный запуск задач поиска вредоносного ПО и обновления.
- Отправка объектов в Sandbox для анализа их поведения в виртуальных операционных системах.
- Получение подробной информации о защите активов.
- Настройка всех компонентов безопасности с помощью приложений "Лаборатории Касперского".

Kaspersky EDR Expert поддерживает иерархию тенантов.

Kaspersky EDR Expert интегрирован с Active Directory, включает API-интерфейсы и поддерживает широкий спектр интеграций как с приложениями "Лаборатории Касперского", так и с решениями сторонних производителей для получения данных и реагирования на них.

Комплект поставки

В состав дистрибутива Kaspersky EDR Expert входят следующие файлы:

- Архив xdr-<номер сборки>-<локаль>.tar, содержащий компоненты Kaspersky EDR Expert, веб-плагины управления, Лицензионные соглашения Kaspersky EDR Expert, KSN и KDT, а также файл legal_notices.
- Архив bin.tar.gz с утилитой KDT, а также шаблоны конфигурационного файла и файла инвентаря KUMA.
- Архив kes_linux_<версия>_local_<номер сборки>.tar, содержащий веб-плагин для Kaspersky Endpoint Security для Linux.
- Архив kesmac_web_plugin_xdr_<номер сборки>.tar, содержащий веб-плагин для Kaspersky Endpoint Security для Mac.

В комплект поставки Kaspersky EDR Expert также входят следующие файлы для развертывания Sandbox:

- Образ диска (файл с расширением iso) с установочными файлами операционной системы Ubuntu Server 22.04 компонента Sandbox.
- Архив с расширением tar.gz компонента Sandbox для создания ISO-образа на базе операционной системы Astra Linux Special Edition 1.8.1.
- Образы дисков (файлы с расширением .iso) операционных систем, в которых компонент Sandbox будет запускать файлы.
- Утилита (файл с расширением .tar) для создания ISO-образа на базе операционной системы Astra Linux Special Edition 1.8.1.

Аппаратные и программные требования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Аппаратные требования для компонентов Kaspersky EDR Expert и Sandbox

Аппаратные требования к компонентам Kaspersky EDR Expert и Sandbox приведены в Руководстве по масштабированию.

Программные требования Kaspersky EDR Expert

Аппаратные и программные требования для OSMP (включая Kaspersky Symphony XDR) см. в справке Kaspersky Symphony XDR.

Требования к программному обеспечению и поддерживаемым системам и платформам

Операционная система	Поддерживаются следующие 64-разрядные версии операционных систем: • Ubuntu Server 24.04 LTS. • Ubuntu Server 26.04 LTS. • Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5).
Среда выполнения	Python 3.8 и выше
Система управления базами данных (СУБД)	PostgreSQL 17.9 64-разрядная. PostgreSQL 18.4 64-разрядная. Postgres Pro 18 Enterprise 64-разрядная (кластер Built-in High Availability). Corosync/Pacemaker поддерживается для всех перечисленных версий PostgreSQL.
Файловая система на узлах кластера (узел контроллера и рабочие узлы)	ext4 XFS

Программные требования для виртуальных платформ

Kaspersky EDR Expert можно развернуть на следующих виртуальных платформах:

- VMware ESXi 7.0.3
- Hyper-V для Windows Server 2022;
- Платформы на базе KVM:
  - ПК СВ "Брест" 3.3;
  - "РЕД Виртуализация" 7.3;
  - zVirt Node 4.5.
- Nutanix 7.5
- Proxmox Virtual Environment 9.1, 9.2

Вы можете развернуть Sandbox на следующих виртуальных платформах:

- VMware ESXi 7.0
- Платформы на базе KVM:
  - ПК СВ "Брест" 3.3;
  - "РЕД Виртуализация" 7.3;
  - zVirt Node 4.2.

Для развертывания компонентов Kaspersky EDR Expert на виртуальной платформе VMware ESXI необходимо установить актуальный пакет обновления для гипервизора.

В случае развертывания компонентов Kaspersky EDR Expert на базе операционной системы Astra Linux в гипервизоре VMware ESXI необходимо обеспечить совместимость используемого серверного оборудования с операционной системой Astra Linux. Полный список поддерживаемого серверного оборудования приведен на сайте разработчика ОС Astra Linux.

Аппаратные и программные требования для приложений Endpoint Agent

Аппаратные и программные требования приложения, используемого в качестве Endpoint Agent, приведены в его документации:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Требования Kaspersky Deployment Toolkit

Все компоненты Kaspersky EDR Expert устанавливаются с помощью утилиты Kaspersky Deployment Toolkit (далее – KDT).

KDT имеет следующие аппаратные и программные требования:

Спецификация	Системные требования
Оборудование	Процессор: 4 ядра, частота от 2500 МГц. Оперативная память: 8 ГБ. Свободное пространство на диске: не менее 100 ГБ, в том числе: • директория хранилища Docker (по умолчанию `/var/lib/docker`): не менее 60 ГБ; • директория временных файлов для KDT (по умолчанию `/tmp`): не менее 15 ГБ.
Операционная система	Поддерживаются следующие 64-разрядные версии операционных систем: • Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5). • Ubuntu Server 24.04 LTS. • Ubuntu Server 26.04 LTS.

Совместимые приложения и решения

Kaspersky EDR Expert 8.3 совместим со следующими приложениями и решениями:

- Kaspersky Security Center Linux 16.2, 16.3 (в качестве подчиненных Серверов администрирования).
- Kaspersky Security Center Windows 14.2, 15.1 (в качестве подчиненных Серверов администрирования).
- Kaspersky Endpoint Security для Windows 12.11.
- Kaspersky Endpoint Security для Windows 12.12.
- Kaspersky Endpoint Security для Windows 14.0.
- Kaspersky Endpoint Security для Windows 14.1.
- Kaspersky Endpoint Security для Linux 12.4.
- Kaspersky Endpoint Security для Linux 12.5.
- Kaspersky Endpoint Security для Mac 12.2.1.
- Kaspersky Private Security Network 3.5.
- Kaspersky Private Security Network 4.0.5.
- Kaspersky Industrial CyberSecurity for Nodes 4.5.
- Kaspersky Managed Detection and Response.

Kaspersky EDR Expert 8.3 можно развернуть на основе компонента OSMP следующих версий:

- Open Single Management Platform 2.3.

Решение Kaspersky EDR Expert 8.3 несовместимо с Sandbox в составе Kaspersky Anti Targeted Attack Platform 8.0.

Архитектура Kaspersky EDR Expert

В этом разделе приведено описание компонентов Kaspersky EDR Expert и их взаимодействия.

В состав Kaspersky EDR Expert входят следующие компоненты:

- Платформа **Open Single Management Platform**, состоящая из следующих частей:
  - **Open Single Management Platform** (OSMP). Технологическая основа, на которой построено решение Kaspersky EDR Expert. OSMP объединяет все компоненты решения и обеспечивает взаимодействие между компонентами. OSMP является масштабируемым и поддерживает интеграцию как с приложениями "Лаборатории Касперского", так и со сторонними решениями.
  - **Консоль OSMP**. Представляет собой веб-интерфейс OSMP.
  - **Incident Response Platform**. Компонент Open Single Management Platform, который позволяет создавать инциденты автоматически или вручную, управлять жизненным циклом алертов и инцидентов, назначать алерты и инциденты аналитикам SOC, а также автоматически или вручную реагировать на инциденты.
  - **Сервер администрирования** (далее также *Сервер*). Ключевой компонент защиты конечных точек организации-клиента. Сервер администрирования обеспечивает централизованное развертывание и управление защитой конечных точек с помощью EPP-приложений, а также позволяет контролировать состояние защиты конечных точек.
  - **OSMP Scanner**. Управляет проверкой объектов с помощью таких технологий обнаружения, как Anti-Malware Engine, YARA и Sandbox.
  - **Сервер агентов**. Этот компонент отвечает за взаимодействие между OSMP и приложениями Endpoint Agent.
  - Компоненты **KUMA**:
    - Ядро KUMA. Центральный компонент KUMA, ответственный за хранение и распространение конфигураций, а также за предоставление графического интерфейса для мониторинга и управления параметрами компонентов KUMA.
    - Коллектор KUMA. Один или несколько коллекторов получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию.
    - Коррелятор KUMA. Анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает алерты в соответствии с правилами корреляции.
    - Хранилище. Обеспечивает хранение нормализованных событий и зарегистрированных инцидентов.
    - Кипер. Критически важный компонент кластера ClickHouse, ответственный за координацию репликации данных в кластере.
- **Sandbox**

  На серверах с компонентом Sandbox запускаются виртуальные машины с образами операционных систем. Компонент Sandbox запускает объекты в этих операционных системах и анализирует поведение объектов для выявления вредоносной активности, признаков целевых атак на IT-инфраструктуру организации.
- **Приложения Endpoint Agents.**

  Endpoint Agent представляет собой программный компонент, устанавливаемый на рабочих станциях и серверах в ИТ-инфраструктуре организации.

В качестве Endpoint Agent может использоваться одно из следующих приложений, в зависимости от операционной системы компьютера:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Приложения Endpoint Agent осуществляют непрерывный мониторинг процессов, активных сетевых соединений и изменения файлов и отправляют полученные данные мониторинга в OSMP.

В таблице ниже перечислены компоненты, входящие в состав Kaspersky EDR Expert.

Компоненты Kaspersky EDR Expert

Название компонента	Описание
`agentserver`	Компонент, позволяющий выполнять действия по реагированию на активах с помощью интеграции с агентами.
`asset-manager`	Компонент для централизованного управления активами.
`backup-operator`	Автоматизированный инструмент, который управляет резервным копированием и восстановлением данных с помощью Custom Resources и меток.
`bootstrap`	Базовая среда выполнения, включающая кластер Kubernetes и компоненты инфраструктуры для работы Kaspersky EDR Expert.
`cp`	Платформа, обеспечивающая обмен данными и взаимодействие между компонентами системы.
`csi-provider`	Компонент, обеспечивающий доступ кластера к внешнему хранилищу через Container Storage Interface (CSI).
`database-cluster`	Набор серверов баз данных, которые работают вместе для обеспечения высокой доступности и масштабируемости.
`database-operator`	Контроллер CloudNativePG Kubernetes для управления конфигурацией подключения к внутренней базе данных, базой данных ресурсов, секретами и ротацией учетных данных.
`gateway`	Шлюз кластера Kubernetes.
`hierman`	Компонент, управляющий операциями иерархии.
`iam`	Компонент платформы OSMP, обеспечивающий аутентификацию и авторизацию.
`irp`	Компонент, который автоматизирует обработку алертов и инцидентов и выполняет действия по реагированию.
`istio`	Сетка служб для управления сервисной связью в кластерах Kubernetes.
`keswin_web_plugin_xdr`	Веб-плагин для управления Kaspersky Endpoint Security for Windows в составе Kaspersky EDR Expert, поддерживающий настройку политики безопасности, отслеживание инцидентов и интеграцию компонентов платформы.
`ksb-facade`	Компонент, обеспечивающий выполнение действий с помощью mixin и шаблонов развертывания.
`ksc`	Сервер администрирования Kaspersky Security Center.
`ksn-proxy-facade`	Компонент, который управляет развертыванием прокси-сервера KSN с помощью Porter, интеграцией внешней службы KSN и обработкой статистики.
`kuma-migrator`	Компонент, автоматизирующий перенос конфигураций, данных и параметров между версиями KUMA.
`loadbalancer`	Компонент, который осуществляет маршрутизацию запросов к контейнерам или процессам в кластере и обеспечивает аудит, аутентификацию и синхронизацию сеансов между узлами.
`nsqlookupd`	Служба, которая обнаруживает отправителей NSQ и направляет клиентов в кластере.
`nwc`	Консоль OSMP.
`objectstorage`	Компонент для хранения временных данных плейбуков, файлов алертов и инцидентов, а также поддержки S3 API для внешних интеграций.

Название компонента	Описание
`observability`	Компонент, обеспечивающий централизованное наблюдение за событиями, угрозами и активами, а также поддерживающий автоматизацию действий по реагированию с помощью интеграции с платформой KUMA.
`orchestra`	Платформа автоматизации. Общий компонент для организации рабочих процессов и выполнения плейбуков для поддержки автоматического реагирования на инциденты и оптимизации операций безопасности.
`osmp-ksn-proxy`	Компонент, который передает статистику обнаружений и алертов в KSN или KPSN с помощью API прокси-сервера KSN и осуществляет маршрутизацию данных.
`osmp-scanner`	Компонент, который выполняет проверку файлов с помощью Anti-Malware, YARA и Sandbox, отправляет их на анализ и формирует отчеты.
`plugin-admin-agent`	Компонент, управляющий политиками Агента администрирования.
`plugin-admin-server`	Компонент, управляющий Серверами администрирования.
`plugin-agent-server`	Компонент, управляющий функциями Kaspersky Endpoint Detection and Response.
`plugin-asset-management`	Компонент, который управляет активами, включая устройства, пользователей и другие ресурсы.
`plugin-enterprise`	Компонент, который интегрируется с другими решениями "Лаборатории Касперского" и обеспечивает управление активами, мониторинг, автоматизацию реагирования и поддержку мультитенантности с помощью веб-интерфейса и API.
`plugin-kata`	Компонент, который интегрируется с KATA/EDR для действий по реагированию, обогащения данных об инцидентах, а также поддержки высокой доступности и масштабируемости.
`plugin-kuma`	Компонент, интегрирующий функции KUMA в Kaspersky EDR Expert.
`plugin-osmp-scanner`	Компонент, который обеспечивает взаимодействие при проверке, интегрируется с Anti-Malware, YARA и Sandbox, отправляет результаты в ObjectStorage, Proxy и Disaster Recovery, а также поддерживает автоматическое и ручное выполнение действий по реагированию.
`plugin-public-api-token-settings`	Компонент, который управляет параметрами API-токена через публичный API для поддержки аутентификации и авторизации для компонентов Kaspersky EDR Expert и внешних систем.
`plugin-tenant-roles`	Компонент, который управляет назначением ролей пользователям и группам пользователей внутри тенантов и интегрируется с IAM для реализации модели пользовательских ролей и поддержки мультитенантности.
`spp_web_plugin_xdr`	Компонент, который интегрируется с плагином Kaspersky Single Product Plugin для управления другими приложениями "Лаборатории Касперского" с помощью Консоли OSMP.
`secrets-manager`	Компонент, который управляет секретами, обеспечивая их безопасное хранение и правильное использование во время развертывания и настройки.
`tenant-registry`	Компонент, управляющий жизненным циклом тенанта, идентификационными данными и интеграцией с серверами Kaspersky Security Center и внешними системами.
`plugin-kessw`	Компонент для управления Kaspersky Embedded Systems Security для Windows (KESS) в составе Kaspersky EDR Expert.
`plugin-kes-linux`	Компонент, который управляет приложением Kaspersky Endpoint Security для Linux.
`plugin-kesw`	Компонент, который управляет приложением Kaspersky Endpoint Security для Windows.
`plugin-spp`	Плагин Kaspersky Single Product Plugin для управления другими приложениями "Лаборатории Касперского" через Консоль OSMP.

Следующие компоненты кластера требуют повышенных привилегий:

Название компонента	Описание
calico	Управляет накладывающей (overlay) сетью.
longhorn	Поддерживает кластерную систему хранения.
local-volume-provisioner	Управляет виртуальными хранилищами.
node-exporter	Проверяет работоспособность кластера.
promtail	Получает диагностическую информацию.
ztunnel	Управляет служебной сетью в накладывающей (overlay) сети.

Целостность образов контейнеров и исполняемых файлов в контейнерах проверяется во время установки путем сопоставления уникального идентификатора хеша SHA256 образа контейнера.

Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к приложению Kaspersky EDR Expert.

Сервер администрирования

Компоненты Kaspersky EDR Expert позволяют осуществлять удаленное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*). Серверы администрирования должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- с именем `kladminserver_srv`;
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью `ksc` либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Полный список параметров установки см. в статье Установка Open Single Management Platform.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов приложений;
- удаленная установка приложений на клиентские устройства и удаление приложений;
- обновление баз и модулей приложений "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе приложений "Лаборатории Касперского";

- распространение лицензионных ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Правило именования Серверов администрирования в интерфейсе приложения

В интерфейсе OSMP Console Серверы администрирования могут иметь следующие имена:

- Имя устройства Сервера администрирования, например: "*имя_устройства*" или "Сервер администрирования: *имя_устройства*".
- IP-адрес устройства Сервера администрирования, например: "*IP_адрес*" или "Сервер администрирования: *IP_адрес*".
- Подчиненные Серверы администрирования и виртуальные Серверы администрирования имеют собственные имена, которые вы указываете при подключении виртуального или подчиненного Сервера администрирования к главному Серверу администрирования.
- Если вы используете приложение OSMP Console, установленное на устройство под управлением Linux, то приложение отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов.

Вы можете подключиться к Серверу администрирования с помощью OSMP Console.

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Корневой Сервер администрирования может действовать только как главный Сервер. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования*.

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить на каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.
- Использование Kaspersky EDR Expert поставщиками услуг. Поставщику услуг достаточно установить Kaspersky EDR Expert и Консоль OSMP. Для управления большим числом клиентских устройств различных организаций поставщик услуг может включать в иерархию Серверов администрирования подчиненные Серверы администрирования (включая виртуальные Серверы).

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

Веб-сервер

Веб-сервер Kaspersky EDR Expert (далее также *Веб-сервер*) – это компонент Kaspersky EDR Expert, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных инсталляционных пакетов.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере. Вы можете передать ссылку пользователю любым удобным способом, например, по электронной почте. По полученной ссылке пользователь может загрузить инсталляционный пакет на локальное устройство.

Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Kaspersky EDR Expert. Агент администрирования требуется установить на все устройства, на которых управление работой приложений "Лаборатории Касперского" выполняется с помощью Kaspersky EDR Expert.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*. Инсталляционный пакет Агента администрирования можно загрузить из следующих источников:

- из хранилища Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования);
- сайт "Лаборатории Касперского".

Агент администрирования для Linux устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Kaspersky Network Agent";
- с автоматическим типом запуска при старте операционной системы;
- с помощью корневой учетной записи.

Агент администрирования для Windows устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- с именем "Kaspersky Security Center Network Agent";
- с автоматическим типом запуска при старте операционной системы;
- с использованием учетной записи LocalSystem.

Агент администрирования для macOS устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- с именем "com.kaspersky.klnagent.core";
- с автоматическим типом запуска при старте операционной системы;
- с использованием корневой учетной записи.

Названия служебных процессов:

- Для Linux:
  - klnagent64.service (для 64-разрядной операционной системы)
  - klnagent.service (для 32-разрядной операционной системы)
- Для Windows:
  - klnagent
- Для macOS:
  - com.kaspersky.klnagent

По умолчанию Агент администрирования устанавливается в следующих директориях:

- Для Linux:
  - для 32-разрядной системы: /opt/kaspersky/klnagent/
  - для 64-разрядной системы: /opt/kaspersky/klnagent64/
- Для Windows:
  - для 32-разрядной системы: C:\Program Files\Kaspersky Lab\NetworkAgent
  - для 64-разрядной системы: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- Для macOS:
  - для 64-разрядной системы: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Для устройств с операционной системой Windows вы можете указать папку для установки Агента администрирования в параметрах инсталляционного пакета. Для устройств с операционной системой Linux Агент администрирования может быть установлен только в директорию по умолчанию.

Папка установки Агента администрирования также содержит утилиты для управления и диагностики работы Агента администрирования, например утилиты klmover и klnagchk.

Во время установки Сервера администрирования, серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования. Для управления устройством с Сервером администрирования рекомендуется установить Агент администрирования для Linux на это устройство. В этом случае Агент администрирования для Linux устанавливается и работает независимо от серверной версии Агента администрирования, которая была установлена вместе с Сервером администрирования.

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (*периодический сигнал*) равным 15 минут на 10 000 управляемых устройств.

Группы администрирования

Группа администрирования (далее также *группа*) – это набор клиентских устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым в Kaspersky EDR Expert.

Для всех управляемых устройств в группе администрирования устанавливаются:

- Единые параметры работы приложений – с помощью групповых политик.
- Единый режим работы всех приложений – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей приложений, проверку устройства по требованию и включение постоянной защиты.

Управляемое устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и управляемые устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести устройство этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, устройству будут автоматически переданы параметры приложений, необходимые для разработчика.

Управляемое устройство

Управляемое устройство – это устройство с операционной системой Linux, Windows или macOS, на котором установлен Агент администрирования. Вы можете управлять такими устройствами с помощью задач и политик для приложений, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Количество устройств, которые могут управляться одним Сервером администрирования, зависит от конфигурации устройства, на котором размещен Сервер администрирования и от ограничений СУБД.

Нераспределенное устройство

Нераспределенное устройство – это устройство в сети, которое не включено ни в одну из групп администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них приложения.

Когда в сети обнаруживается новое устройство, оно помещается в группу администрирования **Нераспределенные устройства**. Можно настроить правила автоматического распределения устройств по группам администрирования в момент обнаружения.

Рабочее место администратора

Устройства, на которых установлен Сервер OSMP Console, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Веб-плагин управления

Веб-плагин управления – это специальный компонент, используемый для удаленного управления приложениями "Лаборатории Касперского" с помощью Консоли OSMP. Веб-плагин управления также называется *плагином управления*. Плагин управления представляет собой интерфейс между Консолью OSMP и определенным приложением "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для приложения.

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач и параметров приложения.
- Интерфейс для создания и изменения политик и профилей политик для удаленной централизованной настройки приложений "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных приложениями.
- Функции Консоли OSMP для отображения оперативных данных и событий приложения, а также статистики, полученной от клиентских устройств.

Политики

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky EDR Expert предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей политик.

Профили политик

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Kaspersky EDR Expert позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

Задачи

Kaspersky EDR Expert управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами OSMP Console, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

> Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Kaspersky EDR Expert как централизованно на Сервере администрирования, так и локально на каждом устройстве.

> Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область действия задачи

Область применения задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал) или DNS-имя. Также можно выбрать устройства, обнаруженные в сети Сервером администрирования.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

  Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Взаимосвязь политики и локальных параметров приложения

Вы можете при помощи политик устанавливать одинаковые значения параметров работы приложения для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров приложения. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт замком).

Значение параметра, которое использует приложение на клиентском устройстве, определяется наличием замка (🔒) у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.
- Если запрет не наложен, то на каждом клиентском устройстве приложение использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры приложения.

Таким образом, при выполнении задачи на клиентском устройстве приложение использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами приложения, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры приложения изменяются после первого применения политики в соответствии с параметрами политики.

Точка распространения

Точка распространения (ранее называлась "агент обновлений") – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в сети.

> Функции и варианты использования Агента администрирования, установленного на устройстве, которое выполняет роль точки распространения, изменяются в зависимости от операционной системы.

Точка распространения может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для точки распространения должна быть создана задача обновления.

  Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.
- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования.

  Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, точку распространения можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

Наличие точки распространения, работающей в режиме шлюза соединений не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

- Осуществлять удаленную установку приложений "Лаборатории Касперского" и других поставщиков программного обеспечения, в том числе установку на клиентские устройства без Агента администрирования.

  Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

- Выступать в роли прокси-сервера, участвующего в Kaspersky Security Network (KSN).

  Можно включить прокси-сервер KSN на стороне точки распространения, чтобы устройство исполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN.

Передача файлов от Сервера администрирования точке распространения осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены точками распространения вручную администратором или автоматически Сервером администрирования. Полный список точек распространения для указанных групп администрирования отображается в отчете со списком точек распространения.

Областью действия точки распространения является группа администрирования, для которой она назначена администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Если точки распространения назначаются автоматически Сервером администрирования, то Сервер назначает точки распространения по широковещательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковещательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковещательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковещательные домены каждые два часа. После того как точки распространения назначены по широковещательным доменам, их невозможно назначить снова по группам администрирования.

Если администратор вручную назначает точки распространения, их можно назначать группам администрирования или сетевым местоположениям.

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.

Kaspersky EDR Expert присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях приложения, изменены не будут.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

Статус точки распространения (*Активный*/*Резервный*) отображается флажком в отчете утилиты klnagchk.

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Kaspersky EDR Expert создает проблему безопасности с уровнем важности *Предупреждение*. Проблема безопасности будет опубликована в свойствах устройства в разделе **Проблемы безопасности**.

При работе задач удаленной установки на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Шлюз соединения

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

- Рекомендуется установить шлюз соединения в демилитаризованной зоне (DMZ). Для других Агентов администрирования, установленных на автономных устройствах, необходимо специально настроить подключение к Серверу администрирования через шлюз соединения.

  Шлюз соединения не изменяет и не обрабатывает данные, передаваемые от Агентов администрирования на Сервер администрирования. Шлюз соединения не записывает эти данные в буфер и, следовательно, не может принимать данные от Агента администрирования и затем передавать их на Сервер администрирования. Если Агент администрирования пытается подключиться к Серверу администрирования через шлюз соединения, но шлюз соединения не может подключиться к Серверу администрирования, Агент администрирования воспринимает это как недоступный Сервер администрирования. Все данные остаются на Агенте администрирования (не на шлюзе соединения).

  Шлюз соединения не может подключиться к Серверу администрирования через другой шлюз соединения. Это означает, что Агент администрирования не может одновременно быть шлюзом соединения и использовать шлюз соединения для подключения к Серверу администрирования.

  Все шлюзы соединения включены в список точек распространения в свойствах Сервера администрирования.

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединения в своей области действия. Однако во внутренней сети шлюзы соединения не дают значительных преимуществ. Они уменьшают количество сетевых подключений, принимаемых Сервером администрирования, но не уменьшают объем входящих данных. Даже без шлюзов соединения все устройства могли подключаться к Серверу администрирования.

Ядро

Ядро – это центральный компонент KUMA, на основе которого строятся все прочие сервисы и компоненты. Предоставляемый Ядром графический пользовательский интерфейс консоли предназначен как для повседневного использования операторами и аналитиками, так и для настройки системы в целом.

Ядро позволяет выполнять следующие задачи:

- создавать и настраивать сервисы (или компоненты) приложения, а также интегрировать в систему необходимое программное обеспечение;
- централизованно управлять сервисами и учетными записями пользователей приложения;
- визуально представлять статистические данные о работе приложения;
- расследовать угрозы безопасности на основе полученных событий.

Хранилище

Хранилище KUMA используется для хранения нормализованных событий таким образом, чтобы к ним обеспечивался быстрый и бесперебойный доступ из KUMA с целью извлечения аналитических данных. Скорость и бесперебойность доступа обеспечивается за счет использования технологии ClickHouse. Таким образом *хранилище* – это кластер ClickHouse, связанный с сервисом хранилища KUMA. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий. Дополнительные сведения см. в документации ClickHouse.

В хранилищах можно создавать *пространства*. Пространства позволяют организовать в кластере структуру данных и, например, хранить события определенного типа вместе.

Коллектор

Коллектор – это компонент приложения, который получает сообщения из источников событий, обрабатывает их и передает в хранилище, коррелятор и/или сторонние сервисы для выявления алертов.

Для каждого коллектора нужно настроить один коннектор и один нормализатор. Вы также можете настроить любое количество дополнительных нормализаторов, фильтров, правил обогащения и правил агрегации. Для того чтобы коллектор мог отправлять нормализованные события в другие сервисы, необходимо добавить точки назначения. Как правило, используются две точки назначения: хранилище и коррелятор.

Алгоритм работы коллектора состоит из следующих этапов:

1. **Получение сообщений из источников событий**

   Для получения сообщений требуется настроить активный или пассивный коннектор. Пассивный коннектор только ожидает события от указанного источника, а активный – инициирует подключение к источнику событий, например к системе управления базами данных.

   Коннекторы различаются по типу. Выбор типа коннектора зависит от транспортного протокола для передачи сообщений. Например, для источника событий, передающего сообщения по протоколу TCP, необходимо установить коннектор типа TCP.

   Доступны следующие типы коннекторов:

   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - diode
   - ftp
   - nfs
   - wmi

- wec
- snmp
- elastic
- etw

2. **Парсинг и нормализация событий**

   События, полученные коннектором, обрабатываются с помощью нормализатора и правил нормализации, заданных пользователем. Выбор нормализатора зависит от формата сообщений, получаемых из источника события. Например, для источника, отправляющего события в формате CEF, необходимо выбрать нормализатор типа CEF.

   Доступны следующие нормализаторы:

   - JSON

3. **Фильтрация нормализованных событий**

   Вы можете настроить фильтры, которые позволят вам выбрать события, соответствующие заданным условиям, для дальнейшей обработки.

4. **Агрегация нормализованных событий**

   Вы можете настроить правила агрегации, чтобы уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор. Настройка правил агрегации позволит объединить несколько событий в одно событие. Это помогает снизить нагрузку на сервисы, которые отвечают за дальнейшую обработку событий, сэкономить место для хранения данных и сэкономить лицензионную квоту (EPS). Например, можно агрегировать в одно событие все события сетевых подключений, выполненных по одному и тому же протоколу транспортного и прикладного уровней между двумя IP-адресами и полученных в течение заданного интервала.

5. **Передача нормализованных событий**

   После завершения всех этапов обработки событие отправляется в настроенные точки назначения.

Коррелятор

Коррелятор – это компонент приложения, который анализирует нормализованные события. В процессе корреляции может использоваться информация из активных листов и/или словарей.

Полученные в ходе анализа данные применяются для выполнения следующих задач:

- управление содержимым активных листов;
- отправка корреляционных событий в настроенные точки назначения.

Корреляция событий выполняется в реальном времени.

Принцип работы коррелятора основан на сигнатурном анализе событий. Это значит, что каждое событие обрабатывается в соответствии с правилами корреляции, заданными пользователем. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает корреляционное событие и отправляет его в Хранилище. Корреляционное событие можно также отправлять на повторный анализ в коррелятор, позволяя таким образом настраивать правила корреляции на срабатывание от предыдущих результатов анализа. Результаты одного правила корреляции могут использоваться другими правилами корреляции.

Вы можете распределять правила корреляции и используемые ими активные листы между корреляторами, разделяя таким образом нагрузку между сервисами. В этом случае коллекторы будут отправлять нормализованные события во все доступные корреляторы.

Алгоритм работы коррелятора состоит из следующих этапов:

1. **Получение события**

   Коррелятор получает нормализованное событие из коллектора или другого сервиса.

2. **Применение правил корреляции**

   Правила корреляции можно настроить на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не был выявлен алерт, обработка события завершается.

3. **Реагирование на алерт**

   Вы можете задать действия, которые приложение будет выполнять при обнаружении алерта. В приложении доступны следующие действия:

   - обогащение события;
   - операции с активными листами;
   - отправка уведомлений;
   - сохранение корреляционного события.

4. **Отправка корреляционного события**

   При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает корреляционное событие и отправляет его в хранилище. На этом обработка события коррелятором завершается.

События

События – это события информационной безопасности, зарегистрированные на контролируемых элементах IT-инфраструктуры организации. Например, события включают попытки входа в систему, взаимодействия с базой данных и многоадресную рассылку информации. Каждое отдельное событие может показаться бессмысленным, но, если рассматривать их вместе, они формируют более широкую картину сетевой активности, которая помогает идентифицировать угрозы безопасности. Это основная функциональность KUMA.

KUMA получает события из журналов и реструктурирует их, приводя данные из разнородных источников к единому формату (этот процесс называется нормализацией). После этого события фильтруются, агрегируются и отправляются в сервис коррелятора для анализа и в сервис хранилища для хранения. Когда KUMA распознает заданное событие или последовательность событий, создаются *корреляционные события*, которые также анализируются и сохраняются. Если событие или последовательность событий указывают на потенциальную угрозу безопасности, KUMA создает алерт. Этот алерт состоит из предупреждения об угрозе и всех связанных данных, которые должен изучить сотрудник службы безопасности.

На протяжении своего жизненного цикла события претерпевают изменения и могут называться по-разному. Так выглядит жизненный цикла типичного события:

Первые шаги выполняются в коллекторе.

1. Сырое событие. Исходное сообщение, полученное KUMA от источника событий с помощью коннектора, называется *"сырым" событием*. Это необработанное сообщение, и KUMA пока не может использовать его. Чтобы с таким событием можно было работать, его требуется нормализовать, то есть привести к модели данных KUMA. Это происходит на следующем этапе.

2. Нормализованное событие. Нормализатор преобразует данные "сырого" события так, чтобы они соответствовали модели данных KUMA. После этой трансформации исходное сообщение становится *нормализованным событием* и может быть проанализировано в KUMA. С этого момента KUMA работает только с нормализованными событиями. Необработанные, сырые события больше не используются, но их можно сохранить как часть нормализованных событий внутри поля `Raw`.

   В приложении представлены следующие нормализаторы:

   - JSON
   - CEF
   - Regexp
   - Syslog (как для RFC3164 и RFC5424)
   - CSV/TSV
   - Ключ-значение
   - XML
   - Netflow v5, v9, IPFIX (v10), sFlow v5
   - SQL

   После завершения этого этапа нормализованные события можно использовать для анализа.

3. Точка назначения. После обработки события коллектором, оно готово к пересылке в другие сервисы KUMA: в коррелятор и/или хранилище KUMA.

Следующие этапы жизненного цикла события проходят в корреляторе.

Типы событий:

1. Базовое событие. Событие, которое было нормализовано.

2. Агрегированное событие. Чтобы не тратить время и ресурсы на обработку большого количества однотипных сообщений, похожие события можно объединять в одно событие. Такие события ведут себя и обрабатываются так же, как и базовые события, но в дополнение ко всем параметрам родительских событий (событий, которые были объединены) агрегированные события имеют счетчик, показывающий количество родительских событий, которые они представляют. Агрегированные события также хранят время, когда были получены первое и последнее родительские события.

3. Корреляционные события. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает *корреляционное событие*. Эти события можно фильтровать, обогащать и агрегировать. Их также можно отправить на хранение или в коррелятор на анализ.

4. Событие аудита. События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью. Эти события используются для обеспечения целостности системы. Они автоматически размещаются в отдельном пространстве хранилища и хранятся не менее 365 дней.

5. Событие мониторинга. Такие события используются для отслеживания изменений в количестве данных, поступающих в KUMA.

Алерты

В KUMA алерты создаются при получении последовательности событий, запускающей правило корреляции. Аналитики KUMA создают правила корреляции для проверки входящих событий на предмет возможных угроз безопасности, поэтому при срабатывании правила корреляции появляется предупреждение о возможной вредоносной активности. Сотрудники службы безопасности, ответственные за защиту данных, должны изучить эти алерты и при необходимости отреагировать на них.

KUMA автоматически присваивает уровень важности каждому алерту. Этот параметр показывает, насколько важны или многочисленны процессы, запустившие правило корреляции. В первую очередь следует обрабатывать алерты с более высоким уровнем важности. Значение уровня важности автоматически обновляется при получении новых корреляционных событий, но сотрудник службы безопасности также может задать его вручную. В этом случае уровень важности алерта больше не обновляется автоматически.

К алертам привязаны относящиеся к ним события, благодаря чему происходит обогащение алертов данными из событий. В KUMA также можно детально анализировать алерты.

На основании алертов можно создать инциденты.

Работа с алертами в KUMA описана в этом разделе.

Инциденты

Если характер поступающих в KUMA данных, создаваемых корреляционных событий и обнаружений указывает на возможную атаку или уязвимость, признаки такого происшествия можно объединить в *инцидент*. Это позволяет экспертам службы безопасности анализировать проявления угрозы комплексно и облегчает реагирование.

Инцидентам можно присваивать категории, типы и уровни важности, а также назначать их сотрудникам, ответственным за защиту данных, для обработки.

Инциденты можно экспортировать в НКЦКИ и MDR.

Ресурсы

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов, на основе которых в свою очередь создаются сервисы KUMA.

Сервисы

Сервисы – это основные компоненты KUMA, с помощью которых осуществляется работа с событиями: получение, обработка, анализ и хранение. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри Консоли KUMA на основе набора ресурсов для сервисов.
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же хранилища могут быть установлены сразу на нескольких устройствах.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Об уровне важности

Параметр *Уровень важности* отражает, насколько чувствительны для безопасности действия, обнаруженные коррелятором KUMA. Он показывает порядок, в котором следует обрабатывать алерты, а также указывает, требуется ли участие старших экспертов по безопасности.

Коррелятор автоматически назначает уровень важности корреляционным событиям и алертам, руководствуясь настройками правил корреляции. Уровень важности алерта также зависит от активов, связанных с обработанными событиями, так как правила корреляции принимают во внимание уровень важности категории этих активов. Если к алерту или корреляционному событию не привязаны активы с уровнем важности или не привязаны активы вообще, уровень важности такого алерта или корреляционного события приравнивается к уровню важности породившего их правила корреляции. Уровень важности алерта или корреляционного события всегда больше или равен уровню важности породившего их правила корреляции.

Уровень важности алерта можно изменить вручную. Измененный вручную уровень важности перестает автоматически обновляться правилами корреляции.

Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Критический

О предоставлении данных

Kaspersky EDR Expert обрабатывает следующие данные:

- Open Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Security Center Linux
- Sandbox
- Приложения Endpoint Agents.

  Подробную информацию о данных, передаваемых приложениями Endpoint Agent, см. в справке соответствующего приложения:

  - Kaspersky Endpoint Security для Windows 12.11.
  - Kaspersky Endpoint Security для Windows 12.12.
  - Kaspersky Endpoint Security для Linux
  - Kaspersky Endpoint Security для Mac

О предоставлении данных

Данные, обрабатываемые локально

Kaspersky EDR Expert предназначен для оптимизации выявления угроз, расследования инцидентов, реагирования (в том числе автоматического), а также проактивного поиска угроз в реальном времени.

Kaspersky EDR Expert выполняет следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- расследование инцидентов и алертов, ручное реагирование;
- автоматическое реагирование с использованием предустановленных и пользовательских плейбуков;
- поиск угроз по событиям в реальном времени.

Для выполнения своих основных функций программа Kaspersky EDR Expert может принимать, хранить и обрабатывать следующую информацию:

- Информация об устройствах, на которые производится установка компонентов Kaspersky EDR Expert:
  - Имя устройства, MAC-адрес, поставщик операционной системы, номер сборки операционной системы, версия ядра ОС, наличие требуемых установленных пакетов, наличие прав для учетной записи, тип средства управления службами, состояние портов. Данная информация собирается Kaspersky Deployment Toolkit при установке.
  - IPv4-адрес. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Имена учетных записей для доступа к устройствам, на которые производится установка компонентов Kaspersky EDR Expert, и SSH ключи. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Имя и пароль учетной записи Kaspersky EDR Expert. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Данные для доступа к СУБД: IP/DNS имя, порт, логин и пароль пользователя. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Файлы инвентаря и лицензии KUMA. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Зона DNS. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Сертификаты безопасного подключения устройств к компонентам Open Single Management Platform. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Гибкая модель статусов инцидентов, включая предустановленные (стандартная или ГОСТ). Наличие модель статусов по ГОСТ настраивается пользователем в конфигурационном файле Kaspersky Deployment Toolkit.

  Информация, которую заполняет пользователь в конфигурационном файле Kaspersky Deployment Toolkit и которую собирает Kaspersky Deployment Toolkit при установке, сохраняется в лог установки, который хранится в базе данных Kaspersky Deployment Toolkit. Лог установки первоначальной инфраструктуры сохраняется в файл на машине пользователя. Срок хранения не ограничен, файл будет удален при деинсталляции решения. Имена пользователей и пароли хранятся в зашифрованном виде.

- Информация о моделях статуса инцидента, включая предустановленную модель.
- Информация о типах инцидентов: общая информация о типе, включая имя и описания типа; связь типа и модели статусов инцидентов.
- Информация об учетных записях пользователей: полное имя и адрес электронной почты. Данная информация вводится пользователем в консоли OSMP. Данные хранятся в базе данных неограниченное время, пока пользователь их не удалит.
- Данные об интеграционном токене.

- Информация о тенантах: название тенанта, название родительского тенанта, описание. Данная информация вводится пользователем в консоли OSMP. Данные хранятся в базе данных неограниченное время, пока пользователь их не удалит.

- Информация о сертификатах: клиентские сертификаты для приложений, которые выполняют роль Endpoint Agent, сертификат сервера OSMP, сертификат сервера KUMA коллектора.

- Информация об устройствах в сети организации.

  - OSMP получает эти данные, если настроена соответствующая интеграция. Активы можно добавлять следующими способами:

    - Импортировать активы:

      - По запросу из MaxPatrol VM.

      - По расписанию: из Kaspersky Security Center Core и Kaspersky Industrial CyberSecurity for Networks.

    - Создать активы вручную в Консоли OSMP или с помощью API.

  - OSMP хранит следующую информацию об устройствах:

    - технические характеристики (общие свойства, ОС, сведения об оборудовании и установленных приложениях "Лаборатории Касперского");

    - обнаруженные уязвимости и статус защиты устройства;

    - данные из конкретных источников;

    - категории устройств и уровни их критичности;

    - AI-рейтинг и AI-статус.

- Данные об алертах и инцидентах:

  - Данные об алертах: сработавшие правила, соответствие матрице MITRE, статус алерта, резолюция, назначенный оператор или группа операторов, затронутые активы (устройства и учетные записи), наблюдаемые объекты (IP, MD5, SHA256, URL, DNS-домен или DNS-имя, имя пользователя, имя хоста), признак наличия устройств КИИ в алерте, комментарии и журнал изменений, файлы. Данная информация формируется в консоли OSMP автоматически на основании корреляционных событий из Kaspersky Unified Monitoring and Analysis Platform.

    - Дополнительные данные также сохраняются в зависимости от типа алерта:

      - для алертов, сформированных по результатам проверки файлов: имена и хеши проверенных файлов; оценки Anti-Malware и Sandbox; информация о действиях с локальными файлами и сетью, инициированных файлом во время анализа в Sandbox; защищенный паролем архив, содержащий проверяемый файловый объект;

      - для алертов, сформированных правилами TAA (IOA) "Лаборатории Касперского": информация о сработавших правилах IOA, описание правил IOA, рекомендации по действиям по реагированию и возможные причины ложных срабатываний (информация о правилах не предоставляется пользователем и распространяется "Лабораторией Касперского");

    - для алертов, генерируемых технологией обнаружения IOC: имена и уровень важности сработавших правил IOC; объекты, обнаруженные во время IOC-проверки устройства, включая IP-адреса, записи DNS, ключи и значения реестра, записи в таблице маршрутизации, информацию о процессах и файлах, сведения о службах, а также имя и идентификатор пользователя;

    - для алертов, генерируемых технологией обнаружения YARA: имена и уровень важности сработавших правил YARA; объекты, обнаруженные во время YARA-проверки устройства, включая информацию о файлах и процессах.

  - Данные об инцидентах: связанные алерты, дочерние инциденты, сработавшие правила, соответствие матрице MITRE, статус инцидента, резолюция, назначенный оператор или группа операторов, затронутые активы (устройства и аккаунты), наблюдаемый объект (из алерта), признак наличия устройств КИИ в инциденте (включая комментарии на графе расследования), журнал изменений, файлы, тип инцидента, метрики по сортировке, реагированию и разрешению инцидентов, and details of the triggered IOA rule, including its name, description, response recommendations, and possible causes of false positives. Данная информация формируется в консоли OSMP автоматически по правилам или вручную пользователем.

  - Данные об инцидентах НКЦКИ: сведения об атакованном ресурсе и о вредоносной системе, информацию из ГосСОПКА по экспортированному инциденту (уникальный идентификатор карточки уведомления в НКЦКИ, регистрационный номер уведомления, дата и время регистрации инцидента в ГосСОПКА, дата последнего обновления инцидента в ГосСОПКА) и журнал изменений. Данная информация формируется автоматически на основании инцидентов XDR для передачи в ГосСОПКА.

  - Данные о настройке правил формирования инцидентов из алертов: имя и условия срабатывания правила, шаблон имени нового инцидента, описание правила, приоритет запуска правила, признак и область наследования. Данная информация вводится пользователем в консоли OSMP.

  - Данные о шаблонах уведомлений: имя шаблона, тема сообщения, шаблон текста сообщения, описание шаблона и правила детектирования, при срабатывании которых будут отправляться уведомления, the selected detection technologies to notify the user about, and the severity of alerts and incidents. Данная информация вводится пользователем в консоли OSMP.

- Данные о настройках сроков хранения алертов и инцидентов

- Граф расследования инцидентов и дерево процессов. OSMP хранит следующую информацию о пользователе о деревьях процессов, построенных для событий: имена созданных деревьев процессов и комментарии.

- Данные о плейбуках:

  - Операционные данные плейбука, в том числе данные о входных параметрах действий по реагированию: название, описание, теги, текст триггера и алгоритма. Данная информация вводится пользователем в консоли OSMP.

  - Данные о результатах выполнения респонсивных действий в рамках исполнения плейбука: содержит данные из интегрированных систем, данные с устройств.

  - Полная история реагирований по всем алертам и инцидентам, including response actions not associated with an alert or incident.

  Перечисленные выше данные о плейбуках хранятся в базе данных в течение трех дней, после чего удаляются. Данные полностью удаляются при деинсталляции Kaspersky EDR Expert.

- Учетные данные для доступа к общим ресурсам. Учетные данные хранятся в зашифрованном виде и распространяются на устройства для поддержки действий по реагированию, таких как получение дампов памяти и образов дисков.

- Информация о файлах, полученных с устройств в результате действий по реагированию или загруженных пользователями вручную, включая имя файла или полный путь к файлу, размер, хеш, тенант, устройство-источник или загрузивший пользователь, описание, статус проверки (Антивирус, YARA, Sandbox) и результаты проверки.

- Информация о правилах запрета, примененных к устройствам. Включает имя правила; хеш; тенант; устройства, к которым применяется правило; статус правила (включено или выключено) и включение уведомлений для пользователя конечного устройства при исполнении файла, соответствующего правилу запрета.

- Информация о правилах YARA, используемых для проверки на устройствах. Включает имя правила; тенант; описание и параметр проверки файлов (включена или выключена), который определяет, будет ли правило применяться при проверке файлов, полученных с устройств или загруженных пользователями, на стороне сервера. Правила хранятся в виде файлов в хранилище объектов OSMP и доставляются на конечные точки при выполнении действия по реагированию для YARA-проверки.

- Информация о правилах IOC, используемых для проверки на устройствах. Включает имя правила, уровень важности, тенант и параметр проверки по расписанию (включена или выключена). Правила хранятся в виде файлов в хранилище объектов OSMP и доставляются на конечные точки при выполнении действия по реагированию для IOC-проверки. При проверке по расписанию на конечные устройства также доставляется расписание проверки, в том числе параметр включения и выключения, время начала проверки и максимальная продолжительность проверки.

- Параметры проверки файловых объектов, включая каталог часто используемых клиентских паролей для расшифровки архивов и источник обновлений для баз данных Управления активами и Sandbox. Параметры настраиваются пользователем в Консоли OSMP.

- При использовании KPSN в OSMP, обрабатываются следующие данные: имя или IP-адрес сервера, на котором развернут KPSN API, а также сертификат, используемый для подключения к API.

- Данные о настройках интеграции (как с программами и службами "Лаборатории Касперского", так и со сторонними решениями, которые участвуют в сценариях Kaspersky EDR Expert):

  - Интеграция с Kaspersky Threat Intelligence Portal: API-токен доступа для подключения к Kaspersky Threat Intelligence Portal, срок хранения кеша, признак подключения через прокси, тип сервиса. Данная информация вводится пользователем в консоли OSMP.

  - Интеграция с НКЦКИ: URL-адрес, API-токен доступа для подключении к ГосСОПКА, наименование компании, сфера деятельности компании, сведения о местонахождении или географическом местоположении информационного ресурса или объекта, признак подключения через прокси. Данная информация вводится пользователем в консоли OSMP.

  - Интеграция с KATA/EDR: адрес сервера KATA/EDR: IP адрес/имя хоста, порт, уникальный идентификатор для подключения к KATA/EDR, файл сертификата и закрытый ключ для подключения к KATA/EDR. Данная информация вводится пользователем в консоли OSMP.

  - Подключение к хосту, где будет запускаться пользовательский скрипт: IP адрес/имя хоста, порт, логин пользователя и SSH ключ, пароль/ключ. Данная информация вводится пользователем в консоли OSMP.

  - Интеграция с Сервером администрирования OSMP: имя Сервера администрирования, полный путь до Сервера администрирования в иерархии. Данная информация вводится пользователем в консоли OSMP.

- Интеграция с Kaspersky Cyber Trace: IPv4/Hostname и порт, по которому доступен Kaspersky Cyber Trace, имя и пароль для подключения. Данная информация вводится пользователем в консоли OSMP.
- Интеграция с Kaspersky Automated Security Awareness Platform (KASAP): API токен доступа при подключении к KASAP, URL портала KASAP, адрес электронной почты администратора KASAP, признак подключения через прокси. Данная информация вводится пользователем в консоли OSMP.
- Интеграция с Active Directory: адреса контроллеров домена, логин и пароль для подключения к контроллерам домена, сертификат. Данная информация вводится пользователем в консоли OSMP.
- Интеграция с внешней системой (например UserGate): данные для подключения к удаленному клиентскому устройству: логин пользователя и SSH ключ, пароль/ключ.
- Интеграция Kaspersky Sandbox: эталонные конфигурации операционных систем виртуальных машин, на которых развернут компонент Sandbox, IP-адрес сервера Sandbox, сертификат сервера Sandbox, имя сервера, отображаемое в Консоли OSMP, и правила Sandbox для анализа файлов. Эта информация вводится пользователем в Консоли OSMP.

- IP-адрес, с которого пользователь подключается к консоли OSMP - фиксируется автоматически консолью, хранится до истечения времени хранения ревизий объектов, которые редактировал пользователь.
- Информация о конфигурации иерархии экземпляров OSMP.

Подробную информацию о прочих данных, принимаемых, хранимых и обрабатываемых для выполнения основных функций решения Kaspersky EDR Expert, см. в справке программ:

- Kaspersky Security Center 15.4 Linux
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky EDR Expert

Перечисленные выше данные хранятся в базе данных, пока пользователь не удалит их. Данные, относящиеся к алерту или инциденту, хранятся в течение всего периода хранения соответствующего алерта или инцидента. Все другие данные хранятся неопределенный срок, пока пользователь не удалит их или не удалит тенант, с которым связаны данные. Эти данные полностью удаляются при деинсталляции Kaspersky EDR Expert.

Все перечисленные выше данные могут быть переданы в "Лабораторию Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Kaspersky EDR Expert, включая файлы журналов, создаваемые инсталляторами и утилитами. Файлы дампов, файлы трассировки или файлы журналов компонентов Kaspersky EDR Expert могут содержать персональные или конфиденциальные данные. Файлы дампов, файлы трассировки или файлы журналов хранятся в открытой форме на устройствах. Файлы дампов, файлы трассировки или файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти файлы в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky EDR Expert. "Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи. Срок хранения данной информации (период ротации) составляет, по умолчанию, 7 дней.

Данные, передаваемые в "Лабораторию Касперского"

Переходя по ссылкам из консоли OSMP к справке Kaspersky EDR Expert, пользователь соглашается на автоматическую передачу в "Лабораторию Касперского" следующих данных: код Kaspersky EDR Expert, версия Kaspersky EDR Expert, локализация Kaspersky EDR Expert.

Для назначения обучающего курса сотруднику Kaspersky EDR Expert передает в Kaspersky Automated Security Awareness Platform (KASAP) следующие данные: email пользователя, ID пользователя в KASAP, ID группы обучения.

Для получения дополнительных данных по алертам Kaspersky EDR Expert передает в Threat Intelligence Portal следующую информацию: тип и значение наблюдаемых объектов из алертов, инцидентов, событий информационной безопасности.

Для получения информации о решении для обнаруженной угрозы при переходе по ссылке из деталей алерта, инцидента или события, Kaspersky EDR Expert передает службе Kaspersky Threats название заключения.

Для получения услуг обнаружения и реагирования на инциденты Kaspersky EDR Expert передает следующие данные службе Kaspersky Managed Detection and Response:

- Если включена интеграция с Kaspersky Managed Detection and Response, OSMP временно сохраняет следующие данные до тех пор, пока они не будут успешно переданы, и передает их в инфраструктуру Kaspersky Managed Detection and Response: идентификатор устройства, на котором сработало правило и было получено событие, идентификатор пользователя и идентификатор клиента Kaspersky Managed Detection and Response.

- При использовании решения Kaspersky Managed Detection and Response из OSMP в инфраструктуру Kaspersky Managed Detection and Response передается следующая дополнительная информация от алертов: имена и значения хеш-функций проверяемых файлов; результаты обнаружения Anti-Malware и Sandbox; информация о локальных действиях файла и сетевой активности, генерируемых файлом при анализе Sandbox; защищенный паролем архив, содержащий проверяемый файловый объект; события, которые запускали IOA-правила, которые могут включать имена файлов и приложений на устройствах, имена и значения разделов реестра, а также имена пользователей.

- При использовании решения Kaspersky Managed Detection and Response от OSMP в инфраструктуру Kaspersky Managed Detection and Response по запросу пользователя передается следующая дополнительная информация: название инцидента; дата и время создания и последнего обновления; информация о сработавших правилах и связанных тактиках и техниках MITRE; имя оператора, назначенного инциденту; имена и идентификаторы затронутых устройств; события, включенные в алерты. Эти события могут включать имена файлов на устройствах клиентов, имена разделов реестра, имена приложений и имена пользователей.

  Все эти данные передаются в Kaspersky Managed Detection and Response только после того, как пользователь принимает Соглашение об обработке данных (DPA) Kaspersky Managed Detection and Response, которое подтверждается при активации Kaspersky Managed Detection and Response в интерфейсе Kaspersky Managed Detection and Response.

Для повышения эффективности защиты информации Kaspersky EDR Expert передает статистику KSN, сгенерированную при работе OSMP, в службу Kaspersky Security Network. Состав передаваемых данных указан в Положении о KSN, которое входит в комплект поставки приложения. Участие в KSN не является обязательным и контролируется пользователем OSMP. Перед передачей статистические данные KSN временно кешируются на серверах, на которых размещены компоненты OSMP.

При использовании Kaspersky Private Security Network статистические данные KSN кешируются на серверах, на которых размещены компоненты OSMP, в том же объеме, что и при использовании Kaspersky Security Network. Если сервер Kaspersky Private Security Network находится за пределами организации, кешированные статистические данные KSN могут быть переданы за пределы организации. Ответственность за обеспечение безопасности этих данных лежит на администраторе Kaspersky Private Security Network.

Данные, передаваемые третьим сторонам

Для получения информации о тактике/технике MITRE при переходе по ссылке из карточки алерта/инцидента, Kaspersky EDR Expert передает на сайт MITRE информацию о тактике/технике: ID и тип.

Для представления информации по инциденту НКЦКИ (Национальный координационный центр по компьютерным инцидентам) в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) Kaspersky EDR Expert передает следующие данные:

- Краткое описание инцидента, категория инцидента, тип инцидента. Дата и время выявления компьютерного инцидента (признака инцидента), начала компьютерной атаки или выявления уязвимости (признака уязвимости), дата и время восстановления штатного режима работы контролируемого информационного ресурса (объекта КИИ) после компьютерного инцидента, окончания компьютерной атаки или устранения уязвимости.
- Наименование главной организации, в которой произошел инцидент. Наименование подчиненной организации, в которой произошел инцидент.
- Ограничительный маркер на распространение сведений из карточки компьютерной атаки, статус реагирования на инцидент.
- Название информационного ресурса, целевая функция или сфера деятельности, в которой функционирует информационный ресурс. Наличие одной из категорий у объекта КИИ или ее отсутствие. Сведения о месте нахождения или географического местоположения информационного ресурса или объекта КИИ. Город, в котором расположен объект КИИ, на котором произошел инцидент, атака или обнаружена уязвимость
- Наименование уязвимого продукта, версия уязвимого продукта.
- Необходимость привлечения сил ГосСОПКА, сведения о средстве или способе выявления инцидента, наличие подключения к сети Интернет.
- Влияние на доступность, влияние на целостность, влияние на конфиденциальность. Описание иной формы последствий компьютерного инцидента или компьютерной атаки
- IPv4-адрес и IPv6-адрес контролируемого ресурса, доменное имя контролируемого ресурса, URI-адрес контролируемого ресурса, Email-адрес контролируемого ресурса.
- Имя атакованной сетевой службы, порт/протокол сетевой службы.
- Тип активности, хеш-сумма вредоносного модуля, описание используемых уязвимостей, идентификатор уязвимости.
- IPv4-адрес и IPv6-адрес вредоносной системы, доменное имя вредоносной системы, URI-адрес вредоносной системы, Email-адрес вредоносной системы.

- AS-Path до атакованной Автономной системы (ASN), номер подставной Автономной системы (ASN), наименование LIR, наименование AS.

- Утечка ПДн, наименование оператора ПДн, ИНН оператора ПДн, адрес оператора ПДн, адрес электронной почты для отправки информации об уведомлении. Предполагаемые причины, повлекшие нарушение прав субъектов ПД. Предполагаемый вред, нанесенный правам субъектов ПД. Характеристики персональных данных, принятые меры по устранению последствий инцидента, информация о результатах внутреннего расследования инцидента, дополнительные сведения.

Для выполнения действий по реагированию через внешние системы (например, UserGate) с помощью выполнения сторонних скриптов на удаленных клиентских устройствах Kaspersky EDR Expert передает во внешние системы следующую информацию: типы и значения наблюдаемых объектов из алертов и инцидентов.

Для проверки репутации файлов и URL при переходе по ссылке из деталей события, Kaspersky EDR Expert передает в сервис VirusTotal следующую информацию: хеши файлов (FileMd5 и FileSha256); имя удаленного устройства (NetUrlHostname); URI точки назначения для HTTP-запросов (NetUri); IPv4-адрес или IPv6-адрес точки назначения (NetDstIp); URL, запрошенный в DNS-запросе (DnsResourceName); и запрошенный DNS-сервер(DnsServerIp).

Предоставление данных в Kaspersky Unified Monitoring and Analysis Platform

Данные, передаваемые третьим сторонам

При использовании функциональности KUMA отсутствует автоматическая передача данных пользователя третьим сторонам.

Данные, обрабатываемые локально

Kaspersky Unified Monitoring and Analysis Platform (далее "KUMA" или "приложение") – это комплексное программное решение, сочетающее в себе следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;

- анализ и корреляция поступающих данных;

- поиск по полученным событиям;

- создание уведомлений о выявлении признаков угроз информационной безопасности;

- создание алертов и инцидентов для обработки угроз информационной безопасности;

- отображение информации о состоянии инфраструктуры заказчика на панели мониторинга и в отчетах;

- мониторинг источников событий;
- управление устройствами (активами): просмотр информации об активах, поиск, добавление, редактирование и удаление активов, экспорт данных об активах в файл формата CSV.

Для выполнения своих основных функций KUMA может принимать, хранить и обрабатывать следующую информацию:

- Данные об устройствах в сети организации.

  Сервер Ядра KUMA получает данные, если настроена соответствующая интеграция. Вы можете добавить активы в KUMA следующими способами:

  - Импортировать активы:
    - По запросу из MaxPatrol VM.
    - По расписанию: из Open Single Management Platform и KICS for Networks.
  - Создать активы вручную через веб-интерфейс или с помощью API.

  KUMA хранит следующие данные об устройствах:

  - Технические характеристики устройства.
  - Уязвимости, обнаруженные на активе.
  - Данные, специфичные для источника получения актива.
- Дополнительные технические характеристики устройств в сети организации, которые пользователь указывает для отправки инцидента в НКЦКИ: IP-адреса, доменные имена, URI-адреса, адрес электронной почты контролируемого объекта, атакованная сетевая служба и порт/протокол.
- Информация об организации: название, ИНН, почтовый адрес, адрес электронной почты для отправки уведомлений.
- Данные Active Directory об организационных единицах, доменах, пользователях, группах, полученные в результате опроса сети Active Directory.

  Сервер Ядра KUMA получает эти данные, если настроена соответствующая интеграция. Для обеспечения безопасного подключения к серверу LDAP пользователь вводит URL сервера, Base DN, учетные данные для подключения и сертификат в Консоли KUMA.
- Данные для доменной аутентификации пользователей в KUMA: корневой DN для поиска групп доступа в службе каталогов Active Directory, URL контроллера домена, сертификат (публичный ключ root, которым подписан сертификат AD), полный путь к группе доступа пользователей в AD (distinguished name).
- Данные, содержащиеся в событиях от настроенных источников

  В коллекторе настраивается источник событий, формируются события KUMA и передаются далее в другие сервисы KUMA. Иногда события могут поступать сначала в сервис агент, который передает события от источника в коллектор. Также вы можете настроить сохранение адреса или имени устройства сервера, который агрегирует события.

  Также агенты Endpoint Agent отправляют в OSMP информацию о событиях в соответствии с моделью данных событий.

- Данные, необходимые для интеграции KUMA с другими приложениями (Kaspersky Threat Lookup, Kaspersky CyberTrace, Open Single Management Platform, Kaspersky Industrial CyberSecurity for Networks, Kaspersky Automated Security Awareness Platform, Kaspersky Endpoint Detection and Response, Security Orchestration, Automation and Response: AI-оценка и статус, Kaspersky Investigation and Response Assistant).

  Это могут быть сертификаты, токены, URL или данные учетной записи для установки соединения с другим приложением, а также другие данные для обеспечения основной функциональности KUMA, например email. Пользователь вводит эти данные в Консоли KUMA.

- Данные об источниках, с которых настроено получение событий.

  Это могут быть название источника, имя устройства, IP-адрес, политика мониторинга, назначенная этому источнику. В политике мониторинга указывается адрес электронной почты ответственного, кому будет отправлено уведомление при нарушении политики.

- Учетные записи пользователей: имя, логин, адрес электронной почты. Пользователь может просмотреть свои данные в профиле в Консоли KUMA.

- Параметры профиля пользователя:

  - Роль пользователя в KUMA. Пользователь может видеть назначенную ему роль.

  - Язык локализации, параметры уведомлений, отображение непечатаемых символов.

    Пользователь вводит эти данные в интерфейсе KUMA.

  - Список категорий активов в разделе **Активы**, панель мониторинга по умолчанию, признак режима ТВ для панели мониторинга, SQL-запрос по событиям по умолчанию, пресет по умолчанию.

    Пользователь указывает эти параметры в соответствующих разделах Консоли KUMA.

- Данные для доменной аутентификации пользователей в KUMA:

  - Active Directory: корневой DN для поиска групп доступа в службе каталогов Active Directory, URL контроллера домена, сертификат (публичный ключ root, которым подписан сертификат AD), полный путь к группе доступа пользователей в AD (distinguished name).

  - Active Directory Federation Services (AD FS): идентификатор доверенной стороны (идентификатор KUMA в AD FS), URI для получения метаданных Connect, URL для перенаправления из AD FS и сертификат сервера AD FS.

  - FreeIPA: Base DN, URL, сертификат (открытый корневой ключ, который использовался для подписи сертификата FreeIPA), пользовательские учетные данные для интеграции, учетные данные для подключения.

- событиях аудита;

  KUMA автоматически фиксирует события аудита.

- Журнал KUMA.

  Пользователь может включить ведение расширенных записей журналов в Консоли KUMA. Записи журнала хранятся на устройстве пользователя, автоматическая передача данных отсутствует.

- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".

- Любые данные, которые пользователь вводит в интерфейсе KUMA.

Перечисленные выше данные могут попасть в KUMA следующими способами:

- Пользователь вводит данные в Консоли KUMA.
- Сервисы KUMA (агент или коллектор) получают данные при настроенном пользователем подключении к источникам событий.
- Через REST API KUMA.
- Данные об устройствах могут быть получены с помощью утилиты из MaxPatrol VM.

Перечисленные данные хранятся в базе данных KUMA (Mongo DB, Click House, SQLite). Пароли хранятся в зашифрованном виде (хранится хеш паролей).

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только в файлах дампа, файлах трассировки или файлах журналов компонентов KUMA, включая файлы журналов, создаваемые установщиком и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов KUMA могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытом виде на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, но администратор может передать эти данные в "Лабораторию Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе KUMA.

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

Предоставление данных в Sandbox

Данные, хранящиеся на сервере с компонентом Sandbox:

- Проверяемые файлы: `/var/opt/kaspersky/sandbox/library/`.
- Результаты проверки файлов: `/var/opt/kaspersky/sandbox/library/` и `/tmp/`.
- Параметры задач: `/var/opt/kaspersky/sandbox/library/` и в базе данных компонента Sandbox.
- Файлы трассировки: `/var/log/kaspersky/sandbox/`.
- Параметры источника обновлений: `/var/opt/kaspersky/apt-updater`.
- Параметры минимальной длины пароля: `/var/opt/kaspersky/apt-config-ram-common/validator.conf`.

- Виртуальные машины: `/vm`.
- Скачанные образы операционных систем и приложений в формате ISO: `/var/opt/kaspersky/sandbox/custom_images/iso`.

Лицензирование

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky EDR Expert.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky EDR Expert.
- Прочитав документ license.txt. Этот документ включен в комплект поставки приложения.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Open Single Management Platform. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Open Single Management Platform или после заказа пробной версии Open Single Management Platform.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Open Single Management Platform или после заказа пробной версии Open Single Management Platform.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

Активация Kaspersky EDR Expert

После установки Kaspersky EDR Expert необходимо выполнить следующие действия:

- Активировать компоненты OSMP.
- Активировать компоненты SIEM.
- Активировать приложения EPP, установленные на устройствах.

Активация компонентов OSMP

Чтобы активировать компоненты OSMP:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

3. В разделе **Действующая лицензия** нажмите на кнопку **Выбрать**.

4. В открывшемся окне выберите лицензионный ключ, который вы хотите использовать для активации компонентов OSMP. Если лицензионного ключа нет в списке, нажмите на кнопку **Добавить лицензионный ключ** и укажите новый лицензионный ключ.

5. При необходимости вы также можете добавить резервный лицензионный ключ. Для этого в разделе **Резервный лицензионный ключ** нажмите на кнопку **Выбрать** и выберите существующий лицензионный ключ или добавьте ключ.

   > Вы не можете добавить резервный лицензионный ключ, если нет активного лицензионного ключа.

6. Нажмите на кнопку **Сохранить**.

Компоненты OSMP активированы.

Активация компонентов SIEM

Компоненты SIEM активируются при активации KUMA.

Чтобы активировать компоненты SIEM:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

2. В открывшемся окне перейдите в **Other** → **License**.

3. Создайте группу лицензионных ключей для вашей лицензии:

   a. Нажмите на кнопку **Добавить лицензионный ключ**.

   b. На панели **Добавить группу** укажите название группы лицензионных ключей.

   c. Нажмите на кнопку **Добавить**.

   Новая группа лицензионных ключей будет добавлена в список **Все лицензионные ключи**.

4. Добавьте лицензионный ключ:

5. Нажмите на имя добавленной группы лицензионных ключей.

6. На панели **Редактирование группы лицензий** выберите нужный вариант, который зависит от того, имеется ли у вас код активации или файл ключа.

   - Чтобы применить код активации:

     a. Нажмите на **Код активации**.

     b. Введите код активации в поле **Код активации**.

     c. Если вы используете Kaspersky EDR Expert в закрытой инфраструктуре, укажите прокси.

     d. Нажмите на кнопку **Загрузить**.

   - Чтобы применить файл ключа:

     a. Нажмите на **Файл ключа**.

     b. В разделе **Активный лицензионный ключ** нажмите на кнопку **Загрузить**, чтобы загрузить файл ключа.

     c. Вы также можете добавить резервный лицензионный ключ, нажав на кнопку **Загрузить** в разделе **Резервный лицензионный ключ**. Обратите внимание, что вы не можете добавить резервный лицензионный ключ, если нет активного лицензионного ключа.

7. Нажмите на кнопку **Add**.

Компоненты SIEM активированы.

Активация приложений EPP

Для активации EPP-программ требуется отдельная лицензия Kaspersky EDR Expert (надстройка Kaspersky Endpoint Detection and Response Expert (on-premises)).

Следующие приложения считаются приложениями EPP:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Чтобы активировать приложения EPP:

1. **Добавьте лицензионный ключ в хранилище Сервера администрирования**

   Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

   1. В главном меню перейдите в раздел **Операции** → **Лицензии**.
   2. Нажмите на кнопку **Добавить**.

3. Выберите то, что вы хотите добавить:

   - **Добавить файл ключа**

     Нажмите на кнопку **Выберите файл ключа** и выберите файл .key, который вы хотите добавить.

   - **Ввести код активации**

     Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет добавлен в хранилище Сервера администрирования.

2. **Распространите лицензионный ключ на клиентские устройства**

Вы можете распространить лицензионный ключ на клиентские устройства с помощью задачи **Добавление ключа**.

Чтобы распространить лицензионный ключ на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.

4. В списке **Тип задачи** выберите задачу **Добавить ключ**.

5. В поле **Название задачи** укажите название новой задачи.

6. Выберите устройства, которым будет назначена задача.

7. На шаге мастера **Выбор лицензионного ключа** перейдите по ссылке **Добавить ключ**, чтобы добавить лицензионный ключ.

8. В панели добавления ключа добавьте лицензионный ключ, используя один из следующих параметров:

   Вам необходимо добавить лицензионный ключ только в том случае, если вы не добавляли его в хранилище Сервера администрирования до создания задачи **Добавление ключа**.

   - Выберите параметр **Ввести код активации**, чтобы ввести код активации, а затем выполните следующие действия:

     a. Укажите код активации и нажмите на кнопку **Отправить**.

     Информация о лицензионном ключе отображается в панели добавления ключа.

     b. Нажмите на кнопку **Сохранить**.

     Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Панель добавления ключа закрыта.

- Выберите параметр **Добавить файл ключа**, чтобы добавить файл ключа, и выполните следующие действия:

  a. Нажмите на кнопку **Выберите файл ключа**.

  b. В открывшемся окне выберите файл ключа и нажмите на кнопку **Открыть**.

  Информация о лицензионном ключе отображается в панели добавления лицензионного ключа.

  c. Нажмите на кнопку **Сохранить**.

  > Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Панель добавления ключа закрыта.

9. Выберите лицензионный ключ в таблице ключей.

10. Если вы хотите заменить активный лицензионный ключ, на шаге мастера **Информация о лицензии** снимите флажок **Использовать в качестве резервного лицензионного ключа**.

    Например, это необходимо, когда организация меняется и на устройстве требуется ключ другой организации или если ключ был перевыпущен и срок действия новой лицензии истекает раньше, чем срок действия текущей лицензии. Чтобы избежать ошибок, снимите флажок **Использовать как резервный лицензионный ключ**.

11. Если на шаге мастера **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

    Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

12. Нажмите на кнопку **Готово**.

    В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо.

Также вы можете автоматически распространять лицензионный ключ на управляемые устройства, если он хранится в хранилище лицензионных ключей Сервера администрирования

Чтобы автоматически распространять лицензионный ключ на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензии**.

2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.

3. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

После активации всех компонентов вы сможете начать использовать Kaspersky EDR Expert.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть информацию об активном и резервном лицензионных ключах:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. В разделе **Тенанты** нажмите на корневой тенант.

   Откроется окно свойств корневого тенанта.

3. Выберите вкладку **Лицензии**.

   Отображается информация об активном и резервном лицензионных ключах.

Отображаемый лицензионный ключ применяется ко всем дочерним тенантам корневого тенанта. Указать отдельный лицензионный ключ для дочернего тенанта невозможно. В окне свойств дочерних тенантов нет вкладки **Лицензии**.

Если лицензионное ограничение ключей превышено, отображается уведомление, а в информации о лицензионном ключе отображается предупреждение.

Вы можете нажать на кнопку **Перейти к Серверу администрирования**, чтобы управлять лицензионными ключами Kaspersky EDR Expert.

Также можно просмотреть список объектов, используемых по лицензии на вкладке **Лицензии**. Для этого нажмите на кнопку ⓘ.

Доступность объекта, используемого по лицензии, зависит от типа приобретенной лицензии.

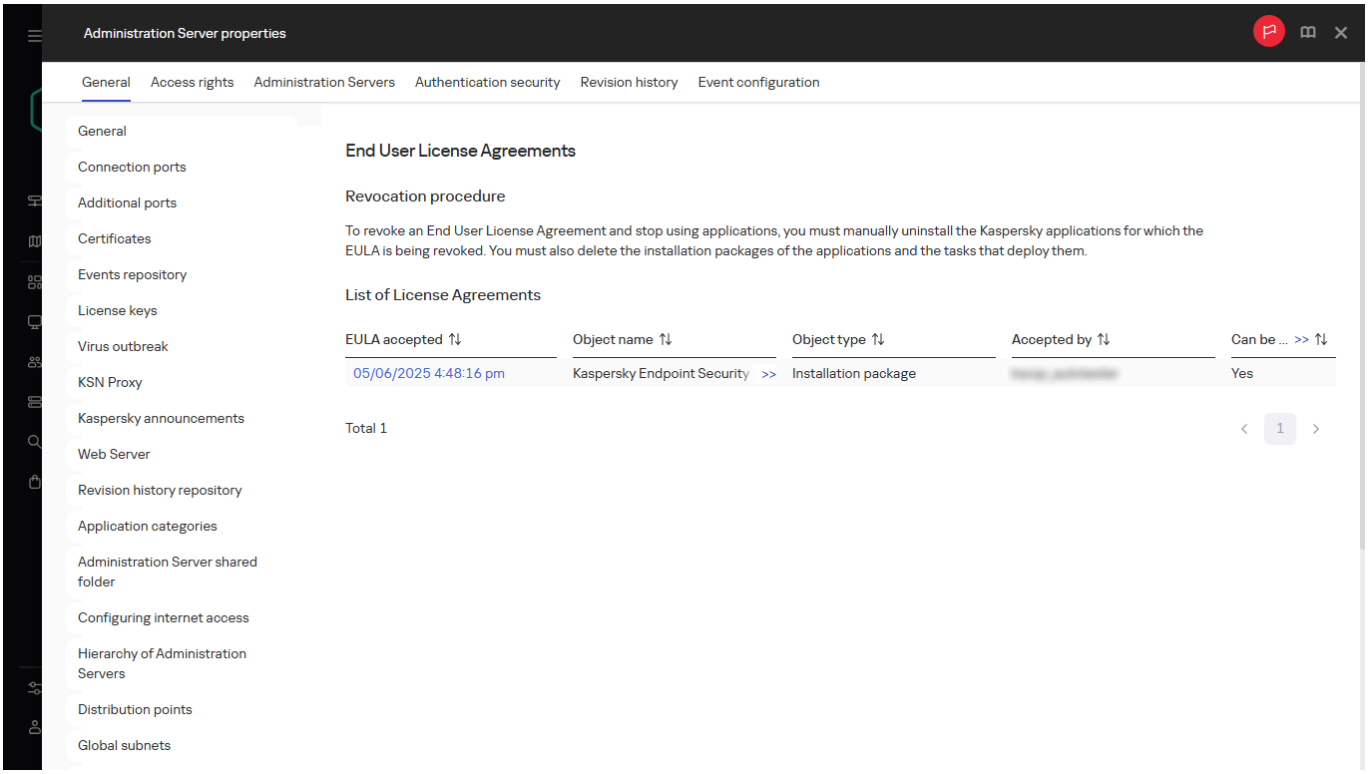
Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любого управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение, прежде чем отзывать его Лицензионное соглашение.

Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":

1. Откройте окно свойств Сервера администрирования и на вкладке **Общие** выберите раздел **Лицензионные соглашения**.

Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.



Список Лицензионных соглашений

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.

3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.
   - Полный текст Лицензионного соглашения.
   - Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; приложение больше не установлено.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии для Kaspersky EDR Expert, а также на входящие в его состав приложения "Лаборатории Касперского", например Kaspersky Unified Monitoring and Analysis Platform. Вы можете продлить лицензии, срок действия которых истек или истекает в течение 30 дней.

Письмо с архивом, содержащим новые лицензионные ключи, будет отправлено на ваш адрес электронной почты после покупки новой лицензии на Kaspersky EDR Expert.

Чтобы продлить срок действия лицензии на Kaspersky EDR Expert:

1. Извлеките новые лицензионные ключи из архива, отправленного на ваш адрес электронной почты.

2. Следуйте инструкциям в разделе Активация Kaspersky EDR Expert.

Срок действия лицензии продлен.

Если вам необходимо продлить лицензии включенных приложений "Лаборатории Касперского", вам нужно добавить лицензионные ключи в веб-интерфейсы этих решений.

О том, как продлить срок действия лицензии для Kaspersky Unified Monitoring and Analysis Platform, см. раздел Добавление лицензионного ключа в веб-интерфейс приложения справки Kaspersky Unified Monitoring and Analysis Platform.

В Консоли Kaspersky SMP уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

Использование Kaspersky Marketplace для выбора бизнес-решений

Marketplace – раздел главного меню, позволяющий просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые вам нужны, и перейти к покупке на сайте "Лаборатории Касперского". Вы можете использовать фильтры для просмотра только тех решений, которые соответствуют вашей организации и требованиям вашей системы информационной безопасности. Когда вы выбираете решение, Kaspersky EDR Expert перенаправляет вас на соответствующую страницу на сайте "Лаборатории Касперского", чтобы вы могли узнать о решении подробнее. Каждая веб-страница позволяет вам перейти к покупке или содержит инструкции по процессу покупки.

В разделе **Marketplace** вы можете фильтровать решения "Лаборатории Касперского" по следующим критериям:

- Количество устройств (конечных точек, серверов и других типов активов), которые вы хотите защитить:
  - 50–250
  - 250–1000
  - Более 1000
- Уровень опытности команды информационной безопасности вашей организации:
  - **Foundations**

    Этот уровень типичен для предприятий, в которых есть только ИТ-команда. Максимально возможное количество угроз блокируется автоматически.
  - **Optimum**

    Этот уровень типичен для предприятий, у которых есть конкретная функция ИТ-безопасности в ИТ-команде. На этом уровне компаниям требуются решения, которые позволят им противостоять товарным угрозам и угрозам в обход существующих превентивных механизмов.
  - **Expert**

    Этот уровень типичен для предприятий со сложной и распределенной ИТ-средой. Группа ИТ-безопасности состоит из опытных специалистов, или в компании есть группа SOC (Security Operations Center). Необходимые решения позволяют компаниям противостоять комплексным угрозам и целевым атакам.
- Типы активов, которые вы хотите защитить:
  - **Конечные точки**: рабочие станции сотрудников, физические и виртуальные машины, встраиваемые системы.
  - **Серверы**: физические и виртуальные серверы.
  - **Cloud**: публичные, частные или гибридные облачные среды; облачные сервисы.
  - **Сеть**: локальная сеть, ИТ-инфраструктура.
  - **Услуга**: услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":

1. В главном окне приложения перейдите в раздел **Marketplace**.

   По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.

3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

Руководство по масштабированию

В этом разделе описаны аппаратные требования для схем развертывания Kaspersky EDR Expert на одном узле и на нескольких узлах.

Для достижения и сохранения оптимальной производительности при различных условиях работы необходимо учитывать количество устройств в сети, топологию сети и требуемый набор функциональных возможностей решения.

Аппаратные и программные требования для OSMP (включая Kaspersky Symphony XDR) см. в справке Kaspersky Symphony XDR.

После выбора сценария развертывания, который лучше всего подходит для вашей IT-инфраструктуры, вы можете рассчитать требования к оборудованию для серверов, на которых размещаются компоненты Kaspersky EDR Expert.

Минимальные требования к оборудованию для небольших конфигураций с числом агентов менее 1000 были увеличены по сравнению с предыдущими версиями Kaspersky EDR Expert. Теперь для работы решения требуется не менее девяти процессорных ядер и 32 ГБ ОЗУ.
Для конфигураций, содержащих более чем 1000 агентов Endpoint Agent, аппаратные требования были снижены.
Схему развертывания на одном узле можно использовать для конфигураций, содержащих до 20 000 агентов Endpoint Agent.
Схему развертывания на нескольких узлах можно использовать для конфигураций, содержащих до 30 000 агентов Endpoint Agent.
Для конфигураций, содержащих более 30 000 агентов Endpoint Agent, необходимо использовать *иерархическую* схему развертывания.

Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.

Расчеты для компонентов Kaspersky EDR Expert

При настройке виртуального диска должен быть выбран тип диска Thick Provision.

Аппаратные требования для компонентов Kaspersky EDR Expert

Аппаратные требования для компонентов Kaspersky EDR Expert зависят от следующих факторов:

- Количество хостов Endpoint Agent:

  Компонент Endpoint Agent может быть установлен на рабочей станции, терминальном сервере, файловом сервере или сетевом хранилище (NAS).

  Для определения эффективного количества хостов с компонентом Endpoint Agent для расчета нагрузки на сервер, можно использовать следующую формулу:

  ```
  K = A+3*B+3*C+20*D
  ```

Здесь:

- "K" - максимальное количество хостов с компонентом Endpoint Agent
- "A" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Windows с установленным компонентом Endpoint Agent.
- "B" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Linux с установленным компонентом Endpoint Agent.
- "C" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы MacOS с установленным компонентом Endpoint Agent.
- "D" – количество серверов.

Допускается использование устройств хранения SSD и HDD. Рекомендуется использовать SSD.

Аппаратные требования для компонентов Kaspersky EDR Expert

Максимальное количество хостов с компонентом Endpoint Agent	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Минимальное количество логических ядер с частотой 2.1 ГГц, низкочастотный процессор	Дисковая подсистема (RAID 10)
1000	56	8	10	6x960 ГБ SSD или 6x1200 ГБ HDD
3000	64	10	14	10x960 ГБ SSD или 8x1200 ГБ HDD
5000	72	12	18	12x960 ГБ SSD или 10x1200 ГБ HDD
10 000	80	18	28	10x1920 ГБ SSD или 8x2400 ГБ HDD
15 000	96	24	36	8x3840 ГБ SSD или 12x2400 ГБ HDD
20 000	128	32	Нет значения	10x3840 ГБ SSD или 16x2400 ГБ HDD

При развертывании Kaspersky EDR Expert на платформах виртуализации увеличьте количество логических ядер, как указано в таблице ниже. Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов, приведенным в таблице выше.

Аппаратные требования для компонентов Kaspersky EDR Expert на платформах виртуализации

Максимальное количество хостов с Endpoint Agent	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер на платформе			Дисковая подсистема (ГБ)
		ESXi, Hyper-V	Другие поддерживаемые платформы на базе KVM (Astra Brest, Red virtualization, zVirt)	Другие поддерживаемые платформы с механизмами защиты от уязвимостей типа Spectre или Meltdown	
1000	56	8	10	12	2530
3000	64	10	14	16	3960
5000	68	14	18	20	5500
10 000	80	20	26	30	9240
15 000	92	28	36	40	12 980
20 000	124	34	44	52	17 270

Аппаратные требования компонентов Kaspersky EDR Expert при развертывании на платформе виртуализации Nutanix приведены в таблице ниже.

Аппаратные требования для компонентов Kaspersky EDR Expert на платформе виртуализации Nutanix

Максимальное количество хостов с компонентом Endpoint Agent	Минимальное количество логических ядер на платформе		Минимальный объем оперативной памяти (ГБ)	Дисковая подсистема (ГБ)
	С защитой от уязвимостей	Без защиты от уязвимостей		
1000	12	10	64	2530
3000	16	14	72	3960
5000	20	18	80	5500
10 000	30	26	88	9240
15 000	40	36	104	12 980
20 000	52	44	136	17 270

Аппаратные требования компонентов Kaspersky EDR Expert при развертывании на платформе виртуализации Proxmox Virtual Environment приведены в таблице ниже.

Аппаратные требования для компонентов Kaspersky EDR Expert на платформе виртуализации Proxmox Virtual Environment

Максимальное количество хостов с компонентом Endpoint Agent	Минимальное количество логических ядер на платформе		Минимальный объем оперативной памяти (ГБ)	Дисковая подсистема (ГБ)
	С защитой от уязвимостей	Без защиты от уязвимостей		
50	10	8	24	1870
100	10	8	24	1870
150	10	8	24	1980
250	10	9	24	1980
500	10	9	28	2200
750	11	10	32	2310
1000	12	10	56	2530
3000	16	14	64	4000
5000	20	18	68	5500
10 000	30	26	80	9240
15 000	40	36	92	12 980
20 000	52	44	124	17 270

Требования к оборудованию для компонентов Kaspersky EDR Expert, развернутых на платформах виртуализации VMware ESXi и Microsoft Hyper-V приведены в таблице ниже. Эти требования применяются к развертываниям, для которых подключено от 50 до 750 агентов Endpoint Agent.

Аппаратные требования для компонентов Kaspersky EDR Expert на платформах виртуализации VMware ESXi и Microsoft Hyper-V с 50–750 агентами Endpoint Agent

Максимальное количество хостов с компонентом Endpoint Agent	Минимальное количество логических ядер на платформе	Минимальный объем оперативной памяти (ГБ)	Дисковая подсистема (ГБ)
50	6	24	1870
100	7	24	1870
150	7	24	1980
250	7	24	1980
500	7	28	2200
750	7	32	2310

Требования к оборудованию для компонентов Kaspersky EDR Expert, развернутых на платформах виртуализации на базе KVM (такие как Astra Brest, Red Virtualization и zVirt), приведены в таблице ниже. Эти требования применяются к развертываниям, для которых подключено от 50 до 750 агентов Endpoint Agent.

Аппаратные требования для компонентов Kaspersky EDR Expert на платформах виртуализации на базе KVM с 50–750 агентами Endpoint Agent

Максимальное количество хостов с компонентом Endpoint Agent	Минимальное количество логических ядер на платформе		Минимальный объем оперативной памяти (ГБ)	Дисковая подсистема (ГБ)
	С защитой от уязвимостей	Без защиты от уязвимостей		
50	10	8	24	1870
100	10	8	24	1870
150	10	8	24	1980
250	10	9	24	1980
500	10	9	28	2200
750	11	10	32	2310

Минимальные значения IOPS (операций ввода-вывода в секунду) для оборудования с развертыванием на одном узле и платформ виртуализации указаны в таблице ниже.

IOPS для оборудования и платформ виртуализации

Максимальное количество хостов с компонентом Endpoint Agent	IOPS (оборудование)	IOPS (виртуализация)
1000	500	500
3000	500	500
5000	700	1000
10 000	1000	1600
15 000	1200	1900
20 000	1400	2200

Требования к каналу связи

Необходимо обеспечить пропускную способность канала связи между сервером Kaspersky EDR Expert и каждым сегментом сети в зависимости от количества хостов Endpoint Agent в сегменте. В таблице ниже указано соответствие пропускной способности канала связи и количества устройств Endpoint Agent, которые не отправляют файлы в Sandbox автоматически.

Соответствие пропускной способности канала связи и количества устройств Endpoint Agent, которые не отправляют файлы в Sandbox автоматически

Максимальное количество хостов Endpoint Agent	Требуемая пропускная способность канала связи, зарезервированная для хостов Endpoint Agent (Мбит/с)
10	2
50	4
100	6
1000	50
10 000	400

Если эффективное количество хостов Endpoint Agent превышает 1000, для расчета требуемой пропускной способности используйте следующую формулу:

```
40 Мбит/с*N:1000
```

где N – количество хостов Endpoint Agent.

Ограничения для расчетов

- Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.
- Размер рассчитан с учетом 30-дневного хранения данных телеметрии.

Расчеты для развертывания Kaspersky EDR Expert на четырех узлах

Для развертывания Kaspersky EDR Expert на нескольких узлах вам потребуется по меньшей мере четыре сервера. В этой статье описывается развертывание Kaspersky EDR Expert на четырех узлах. Требования к этим серверам зависят от того, будут ли компоненты Kaspersky EDR Expert развернуты на физических серверах или виртуальных платформах.

Развертывание компонентов Kaspersky EDR Expert на физических серверах

Требования к серверам

Максимальное количество хостов с компонентом Endpoint Agent	Минимальный объем оперативной памяти (ГБ)				Минимальное количество логических ядер			
	Узел контроллера	Рабочий узел 1	Рабочий узел 2	Рабочий узел 3	Узел контроллера	Рабочий узел 1	Рабочий узел 2	Рабочий узел 3
1000	8	24	24	40	6	6	4	6
3000	8	24	24	40	6	6	6	8
5000	8	24	24	40	6	8	6	8
10 000	8	24	24	48	6	10	8	10
15 000	8	32	24	56	6	12	10	12
20 000	8	56	32	64	6	16	10	12
30 000	8	112	40	72	6	20	14	16

Допускается использование устройств хранения SSD и HDD. Рекомендуется использовать SSD.

Требования к месту на диске

Максимальное количество хостов с компонентом Endpoint Agent	Дисковая подсистема			
	Управляющий узел (RAID 1)	Рабочий узел 1 (RAID 10)	Рабочий узел 2 (RAID 10)	Рабочий узел 3 (RAID 10)
1000	2x960 ГБ SSD или 2x600 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD
3000	2x960 ГБ SSD или 2x600 ГБ HDD	6x960 ГБ SSD или 4x1200 ГБ HDD)	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD
5000	2x960 ГБ SSD или 2x600 ГБ HDD	8x960 ГБ SSD или 8x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD

Максимальное количество хостов с компонентом Endpoint Agent	Дисковая подсистема			
	Управляющий узел (RAID 1)	Рабочий узел 1 (RAID 10)	Рабочий узел 2 (RAID 10)	Рабочий узел 3 (RAID 10)
10 000	2x960 ГБ SSD или 2x600 ГБ HDD	10x1920 ГБ SSD или 8x2400 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD
15 000	2x960 ГБ SSD или 2x600 ГБ HDD	8x3840 ГБ SSD или 10x2400 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD
20 000	2x960 ГБ SSD или 2x600 ГБ HDD	8x3840 ГБ SSD или 14x2400 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	6x960 ГБ SSD или 4x1200 ГБ HDD
30 000	2x960 ГБ SSD или 2x600 ГБ HDD	12x3840 ГБ SSD или 16x2400 ГБ HDD	4x960 ГБ SSD или 4x1200 ГБ HDD	8x960 ГБ SSD или 6x1200 ГБ HDD

Развертывание компонентов Kaspersky EDR Expert на платформах виртуализации

Требования для VMware ESXi и Microsoft Hyper-V

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		Рабочий узел 1		Рабочий узел 2		Рабочий узел
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)
1000	8	6	24	6	24	6	40
3000	8	6	24	8	24	6	40
5000	8	6	24	8	24	6	40
10 000	8	6	24	12	24	8	48
15 000	8	6	32	14	24	10	52
20 000	8	6	56	16	32	12	60
30 000	8	6	116	22	40	14	72

Требования для платформ на базе KVM (Astra Brest, Red Virtualization, zVirt)

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		Рабочий узел 1		Рабочий узел 2		Рабочий узел
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)
1000	8	6	24	8	24	6	36
3000	8	6	24	10	24	8	40
5000	8	6	24	10	24	8	40
10 000	8	6	24	14	24	10	48
15 000	8	6	32	18	24	12	52
20 000	8	6	56	22	32	14	60
30 000	8	6	116	28	40	20	72

Требования для платформ виртуализации Proxmox Virtual Environment и Nutanix

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		Рабочий узел 1		Рабочий узел 2		Рабочий узел
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
1000	8	6	24	8	24	6	36	
3000	8	6	24	10	24	8	40	
5000	8	6	24	10	24	8	40	
10 000	8	6	24	14	24	10	48	
15 000	8	6	32	18	24	12	52	
20 000	8	6	56	22	32	14	60	
30 000	8	6	116	28	40	20	72	

При использовании платформы со средствами защиты от уязвимостей типа Spectre или Meltdown необходимо настроить количество логических ядер в соответствии с таблицей ниже.

Количество логических ядер, которые требуются для узлов с защитой от уязвимостей типа Spectre и Meltdown

Максимальное количество хостов с компонентом Endpoint Agent	Минимальное количество логических ядер			
	Узел контроллера	Рабочий узел 1	Рабочий узел 2	Рабочий узел 3
1000	6	10	8	12
3000	6	10	8	12
5000	6	12	10	14
10 000	6	16	12	16
15 000	6	20	14	18
20 000	6	24	18	20
30 000	6	34	22	26

Требования к дисковому пространству (все платформы виртуализации, ГБ)

Максимальное количество хостов с компонентом Endpoint Agent	Дисковая подсистема			
	Узел контроллера	Рабочий узел 1	Рабочий узел 2	Рабочий узел 3
1000	537	1210	1100	1870
3000	537	2640	1100	1870
5000	537	4179	1100	1870
10 000	537	7917	1100	1870
15 000	537	11 655	1100	1870
20 000	537	15 394	1100	2309
30 000	537	22 870	1100	3300

Ограничения для расчетов

- Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.
- Размер рассчитан с учетом 30-дневного хранения данных телеметрии.

Расчеты для развертывания Kaspersky EDR Expert на шести узлах

Для развертывания Kaspersky EDR Expert на нескольких узлах вам потребуется по меньшей мере четыре сервера. В этой статье описывается развертывание Kaspersky EDR Expert на шести узлах. Требования к этим серверам зависят от того, будут ли компоненты Kaspersky EDR Expert развернуты на физических серверах или виртуальных платформах.

Развертывание компонентов Kaspersky EDR Expert на физических серверах

Требования к серверам

Максимальное количество хостов с компонентом Endpoint Agent	Минимальный объем оперативной памяти (ГБ)					Минимальное количество логических			
	Узел контроллера	3 рабочих узла	Узел базы данных (PostgresSQL)	Узел сервиса KUMA	2 узла с хранилищами KUMA	Узел контроллера	3 рабочих узла	Узел базы данных (PostgresSQL)	Узел серви KUM
1000	8	24	16	32	Нет значения	6	8	6	16
3000	8	24	16	32	Нет значения	6	10	6	16
5000	8	24	16	32	Нет значения	6	10	6	16
10 000	8	24	16	32	Нет значения	6	10	6	16
15 000	8	24	24	32	Нет значения	6	10	6	16
20 000	8	24	24	56	Нет значения	6	12	6	16
30 000	8	32	32	32	64	6	14	8	16
50 000	8	32	48	48	96	6	16	12	16

Допускается использование устройств хранения SSD и HDD. Настоятельно рекомендуется использовать SSD.

Требования к месту на диске

Максимальное количество хостов с компонентом Endpoint Agent	Дисковая подсистема				
	Управляющий узел (RAID 1)	3 рабочих узла (RAID 10)	Узел базы данных (PostgresSQL, RAID 10)	Узел сервисов KUMA (RAID 10)	2 узла с хранилищами KUMA
1000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	Нет значения
3000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	6x960 ГБ SSD	Нет значения
5000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	8x960 ГБ SSD	Нет значения
10 000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	8x1920 ГБ SSD	Нет значения
15 000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	12x1920 ГБ SSD	Нет значения
20 000	2x960 ГБ SSD	4x960 ГБ SSD	6x960 ГБ SSD	8x3840 ГБ SSD	Нет значения
30 000	2x960 ГБ SSD	4x960 ГБ SSD	6x960 ГБ SSD	4x960 ГБ SSD	12x1920 ГБ SSD
50 000	2x960 ГБ SSD	4x960 ГБ SSD	10x1920 ГБ SSD	4x960 ГБ SSD	10x3840 ГБ SSD

Развертывание компонентов Kaspersky EDR Expert на платформах виртуализации

Требования для VMware ESXi и Microsoft Hyper-V

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		3 рабочих узла		Узел базы данных (PostgresSQL)		Узел сервиса KU	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
1000	8	6	24	10	12	6	32	
3000	8	6	24	10	12	6	32	
5000	8	6	24	10	12	6	32	
10 000	8	6	24	12	16	6	32	
15 000	8	6	24	12	20	6	32	
20 000	8	6	28	12	24	6	52	
30 000	8	6	28	14	32	8	32	
50 000	8	6	32	18	48	12	44	

Требования для платформ на базе KVM (Astra Brest, Red Virtualization, zVirt)

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		3 рабочих узла 1		Узел базы данных (PostgresSQL)		Узел сервиса KU	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
1000	8	6	24	12	12	6	32	
3000	8	6	24	12	12	6	32	
5000	8	6	24	14	12	6	32	
10 000	8	6	24	14	16	6	32	
15 000	8	6	24	16	20	6	32	
20 000	8	6	28	14	24	8	52	
30 000	8	6	28	18	32	10	32	
50 000	8	6	32	22	48	16	44	

Требования для платформ виртуализации Proxmox Virtual Environment и Nutanix

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		3 рабочих узла 1		Узел базы данных (PostgresSQL)		Узел сервиса KU	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
1000	8	6	24	12	12	6	32	
3000	8	6	24	12	12	6	32	
5000	8	6	24	14	12	6	32	
10 000	8	6	24	14	16	6	32	
15 000	8	6	24	16	20	6	32	
20 000	8	6	28	16	24	8	52	

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера		3 рабочих узла 1		Узел базы данных (PostgresSQL)		Узел сервиса KU	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин кол ло
30 000	8	6	28	18	32	10	32	
50 000	8	6	32	22	48	16	44	

При использовании платформы со средствами защиты от уязвимостей типа Spectre или Meltdown необходимо настроить количество логических ядер в соответствии с таблицей ниже.

Количество логических ядер, которые требуются для узлов с защитой от уязвимостей типа Spectre и Meltdown

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера	3 рабочих узла	Узел базы данных (PostgresSQL)	Узел сервиса KUMA	2 узла с хранилищами KUMA
1000	6	14	6	16	Нет значения
3000	6	14	6	16	Нет значения
5000	6	16	6	16	Нет значения
10 000	6	16	6	16	Нет значения
15 000	6	18	8	16	Нет значения
20 000	6	18	8	20	Нет значения
30 000	6	22	12	16	24
50 000	6	26	18	22	32

Требования к дисковому пространству (все платформы виртуализации, ГБ)

Максимальное количество хостов с компонентом Endpoint Agent	Узел контроллера	3 рабочих узла	Узел базы данных (PostgresSQL)	Узел сервиса KUMA	2 узла с хранилищами KUMA
1000	537	1100	1540	1100	Нет значения
3000	537	1100	1540	2309	Нет значения
5000	537	1100	1540	3519	Нет значения
10 000	537	1100	1540	6817	Нет значения
15 000	537	1100	1540	9896	Нет значения
20 000	537	1100	1980	13 085	Нет значения
30 000	537	1100	2859	1100	9896
50 000	537	1100	4728	1100	16 273

Ограничения для расчетов

- Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.
- Размер рассчитан с учетом 30-дневного хранения данных телеметрии.

Расчеты для конфигурации кластера высокой доступности

Для развертывания в отказоустойчивой конфигурации необходимы следующие серверы:

- 3 контроллера. Отказоустойчивая кластерная конфигурация может предусматривать от одного до трех узлов контроллера. Рекомендуется использовать три узла контроллера.
- 4 рабочих узла.
- 2 узла хранения.
- 2 узла с коллектором KUMA.
- 2 узла с коррелятором KUMA.
- 3 узла базы данных (PostgresSQL).

Характеристики узлов приведены в таблицах ниже.

Развертывание на физических серверах

Минимальный объем оперативной памяти и количество логических ядер

Максимальное количество хостов с компонентом Endpoint Agent	Минимальный объем оперативной памяти (ГБ)						Минима		
	3 узла контроллера	4 рабочих узла	3 узла базы данных (PostgresSQL)	2 узла с коллектором KUMA	2 узла с коррелятором KUMA	2 узла хранения ClickHouse	3 узла контроллера	4 рабочих узла	3 у (Pos
1000	8	24	16	16	16	64	6	8	
3000	8	24	16	16	16	64	6	10	
5000	8	24	16	16	16	64	6	10	
10 000	8	24	16	16	16	64	6	10	
15 000	8	24	24	16	16	64	6	10	
20 000	8	24	24	24	16	96	6	12	
30 000	8	32	32	24	16	128	6	14	
50 000	8	32	48	40	16	256	6	16	

Допускается использование устройств хранения SSD и HDD. Рекомендуется использовать SSD.

Требуемое место на диске

Максимальное количество хостов с компонентом Endpoint Agent	3 узла управления (RAID 1)	4 рабочих узла (RAID 10)	3 узла базы данных (PostgresSQL) (RAID 10)	1 узел коллектора KUMA (RAID 10)	1 узел коррелятора KUMA	2 узла хранилища ClickHouse
1000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	4x960 ГБ SSD
3000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	6x960 ГБ SSD
5000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	8x960 ГБ SSD
10 000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	8x1920 ГБ SSD
15 000	2x960 ГБ SSD	4x960 ГБ SSD	4x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	12x1920 ГБ SSD
20 000	2x960 ГБ SSD	4x960 ГБ SSD	6x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	8x3840 ГБ SSD
30 000	2x960 ГБ SSD	4x960 ГБ SSD	6x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	12x3840 ГБ SSD
50 000	2x960 ГБ SSD	4x960 ГБ SSD	10x960 ГБ SSD	2x960 ГБ SSD	2x960 ГБ SSD	10x7680 ГБ SSD

Развертывание на платформах виртуализации

Минимальный объем оперативной памяти и количество логических ядер для ESXi и Microsoft Hyper-V

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера		4 рабочих узла		3 узла базы данных (PostgresSQL)		1 узел коллектора	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин кол ло
1000	8	6	24	10	12	6	16	
3000	8	6	24	10	12	6	16	
5000	8	6	24	10	12	6	16	
10 000	8	6	24	12	16	6	16	
15 000	8	6	24	12	20	6	16	
20 000	8	6	28	12	24	6	20	
30 000	8	6	28	14	32	8	24	
50 000	8	6	32	18	48	12	36	

Минимальный объем оперативной памяти и количество логических ядер для платформ на базе KVM (Astra Brest, Red Virtualization и zVirt)

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера		4 рабочих узла		3 узла базы данных (PostgresSQL)		1 узел коллектора	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин кол ло
1000	8	6	24	14	12	6	16	
3000	8	6	24	14	12	6	16	
5000	8	6	24	14	12	6	16	
10 000	8	6	24	14	16	6	16	

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера		4 рабочих узла		3 узла базы данных (PostgresSQL)		1 узел коллектора	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
15 000	8	6	24	14	20	6	16	
20 000	8	6	28	16	24	8	20	
30 000	8	6	28	18	32	10	24	
50 000	8	6	32	22	48	16	36	

Минимальный объем оперативной памяти и количество логических ядер для платформ виртуализации Proxmox Virtual Environment и Nutanix

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера		4 рабочих узла		3 узла базы данных (PostgresSQL)		2 узла коллектора	
	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальный объем оперативной памяти (ГБ)	Мин ко ло
1000	8	6	24	12	12	6	16	
3000	8	6	24	12	12	6	16	
5000	8	6	24	14	12	6	16	
10 000	8	6	24	14	16	6	16	
15 000	8	6	24	16	20	6	16	
20 000	8	6	28	16	24	8	20	
30 000	8	6	28	18	32	10	24	
50 000	8	6	32	22	48	16	36	

При активных средствах устранения уязвимостей необходимо изменить количество логических ядер в соответствии с таблицей ниже.

Минимальное количество логических ядер при активных средствах устранения уязвимостей

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера	4 рабочих узла	3 узла базы данных (PostgresSQL)	1 узел коллектора KUMA	1 узел с коррелятором KUMA	2 узла хранения ClickHouse
1000	6	14	6	8	8	24
3000	6	14	6	8	8	24
5000	6	16	6	8	8	24
10 000	6	16	6	8	8	24
15 000	6	18	8	8	8	24
20 000	6	18	8	10	8	32
30 000	6	22	12	14	8	32
50 000	6	26	18	22	8	48

Требуемое место на диске для платформ виртуализации

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера	4 рабочих узла	3 узла базы данных (PostgresSQL)	1 узел коллектора KUMA	1 узел с коррелятором KUMA	2 узла хранения ClickHouse
1000	537	1100	1540	645	645	1100
3000	537	1100	1540	645	645	2309
5000	537	1100	1540	645	645	3519
10 000	537	1100	1540	645	645	6817

Максимальное количество хостов с компонентом Endpoint Agent	3 узла контроллера	4 рабочих узла	3 узла базы данных (PostgresSQL)	1 узел коллектора KUMA	1 узел с коррелятором KUMA	2 узла хранения ClickHouse
15 000	537	1100	1540	645	645	9896
20 000	537	1100	1980	645	645	13 085
30 000	537	1100	2860	645	645	19 462
50 000	537	1100	4728	645	645	32 216

Ограничения для расчетов

- Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.
- Размер рассчитан с учетом 30-дневного хранения данных телеметрии.

Расчеты для Sandbox

Аппаратные требования к серверу с компонентом Sandbox зависят от типа и объема обрабатываемого трафика и от допустимого времени проверки объекта.

Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.

Работа компонента Sandbox не поддерживается на процессорах AMD.

Количество физических серверов с компонентом Sandbox, которое требуется для проверки файлов

Требуемое количество физических серверов с компонентом Sandbox, которое зависит от количества подключенных агентов Endpoint Agent (см. таблицу ниже).

Необходимое количество физических серверов с компонентом Sandbox

Максимальное количество хостов с компонентом Endpoint Agent	Отправка файлов на анализ из Endpoint Agent в интеграцию Sandbox отключена	Отправка файлов на анализ из Endpoint Agent в интеграцию Sandbox включена
1000	1	1
3000	1	2
5000	1	3
10 000	1	4
15 000	1	5

Аппаратные требования к серверу с компонентом Sandbox

Одного сервера Sandbox с установленной операционной системой по умолчанию будет достаточно, если агенты Endpoint Agent не отправляют файлы в Sandbox автоматически.

При установке компонента Sandbox на виртуальную машину VMware ESXi с процессором 2,1 ГГц вам потребуется в семь раз больше виртуальных серверов для достижения такой же производительности, как у одного физического сервера.

Для виртуальных платформ на базе KVM, таких как "Брест", "РЕД Виртуализация" или zVirt Node, вам потребуется в 13 раз больше виртуальных серверов.

В этих расчетах учитывается необходимость поддержания настроенного времени проверки объектов.

При установке компонента Sandbox на виртуальной платформе на базе KVM, такой как "Брест", "РЕД Виртуализация" или zVirt Node, при активных средствах устранения уязвимостей типа Spectre и Meltdown потребуется в 19 раз больше серверов. В этих расчетах учитывается необходимость настроить время проверки объектов.

Если вы используете пользовательские образы для серверов с компонентом Sandbox, могут потребоваться дополнительные мощности.

Расчет количества физических серверов с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно пользовательским правилам Sandbox, в час> * <количество пользовательских образов операционных систем> / 1000
```

Расчет количества виртуальных машин VMware ESXi с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно пользовательским правилам Sandbox, в час> * <количество пользовательских образов операционных систем> / 142
```

При установке компонента Sandbox на виртуальные платформы на базе KVM, такие как "Брест" или zVirt Node, расчет количества виртуальных машин, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество физических серверов с компонентом Sandbox> * 13
```

При установке компонента Sandbox на виртуальную платформу "РЕД Виртуализация" расчет количества виртуальных машин, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество физических серверов с компонентом Sandbox> * 13
```

Оценка количества серверов Sandbox приведена для серверов следующей конфигурации:

- При установке компонента Sandbox на физический сервер:
  - Процессора Intel Xeon 16 Core (HT) с частотой 2,6 ГГц или выше.
  - 80 ГБ оперативной памяти.
  - 2 HDD объемом 600 ГБ каждый, объединенные в массив RAID 1.
  - При установке компонента Sandbox на физический сервер с приведенной выше конфигурацией вам нужно установить ограничение для количества одновременно запускаемых виртуальных машин – 48.
- При установке компонента Sandbox на виртуальную машину:
  - 15 виртуальных процессоров с частотой 2,1 ГГц или выше.

    При установке компонента Sandbox на виртуальные платформы на базе KVM, такие как "Брест", zVirt Node и "РЕД Виртуализация", для оптимальной производительности рекомендуется использовать процессоры Intel поколения Ice Lake и выше.
  - 32 ГБ оперативной памяти.
  - HDD объемом 645 ГБ.

    На виртуальной машине:
    - Разрешена вложенная виртуализация.
    - Установлены параметры High Latency Sensitivity (только при установке на виртуальную машину VMware ESXi).
    - Зарезервирована вся оперативная память.
    - Зарезервирована вся частота процессора.

  При установке компонента Sandbox на виртуальную машину с приведенной выше конфигурацией вам нужно установить ограничение для количества одновременно запускаемых виртуальных машин – 12.

Если вы планируете использовать пользовательские образы операционных систем, рекомендуется увеличить объем дискового пространства до 600 ГБ и больше.

Ограничения для расчетов

Аппаратные требования указаны приблизительно. Чтобы получить более точную оценку требований, в которой учтены все сценарии, обратитесь в Службу технической поддержки.

Развертывание Kaspersky EDR Expert

Следуя этому сценарию, вы можете подготовить инфраструктуру к развертыванию Open Single Management Platform и всех необходимых компонентов для Kaspersky EDR Expert (включая функциональность Kaspersky Endpoint Detection and Response), подготовить конфигурационный файл, содержащий параметры установки, и развернуть решение с помощью утилиты Kaspersky Deployment Toolkit (далее также KDT).

Прежде чем приступить к развертыванию Open Single Management Platform и компонентов Kaspersky EDR Expert, рекомендуется прочитать Руководство по усилению защиты.

Сценарий развертывания состоит из следующих этапов:

1. **Выбор варианта развертывания Kaspersky EDR Expert**

   Выберите конфигурацию Kaspersky EDR Expert, наиболее подходящую для вашей организации. Доступно развертывание на одном узле, на четырех узлах, на шести узлах и на 14 узлах (отказоустойчивая конфигурация).

2. **Загрузка дистрибутива с компонентами Kaspersky EDR Expert**

   В состав дистрибутива входят следующие компоненты:

   - Транспортный архив, который содержит компоненты Kaspersky EDR Expert и Лицензионные соглашения Kaspersky EDR Expert и KDT.

     Компоненты подписаны ключом RSA и ключом ГОСТ Р 34.11-2012. Вы можете проверить подлинность и целостность компонентов Kaspersky EDR Expert.

   - Архив с утилитой KDT, а также шаблоны конфигурационного файла и файл инвентаря KUMA.

3. **Установка системы управления базами данных (СУБД)**

   Для развертывания на нескольких узлах вручную установить СУБД на отдельный сервер, который не будет включен в кластер Kubernetes.

   Для развертывания на одном узле вручную установите СУБД на целевом устройстве перед развертыванием Kaspersky EDR Expert. В этом случае компоненты СУБД и Kaspersky EDR Expert устанавливаются на одном и том же целевом устройстве, но СУБД не будет включена в кластер Kubernetes.

4. **Подготовка устройства администратора и целевых устройств**

   С учетом выбранной схемы развертывания определите количество целевых устройств, на которых вы будете разворачивать кластер Kubernetes и компоненты Kaspersky EDR Expert, входящие в этот кластер. Подготовьте выбранные устройство администратора и целевые устройства к развертыванию Kaspersky EDR Expert.

   Инструкции:

   - Развертывание на нескольких узлах: подготовка устройства администратора и целевых устройств
   - Развертывание на одном узле: подготовка устройства администратора и целевых устройств

5. **Подготовка устройств KUMA для установки сервисов KUMA вне кластера Kubernetes (не обязательно)**

   Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера Kubernetes, на отдельных хостах вне кластера или частично в кластере и вне его.

Если вы хотите полностью установить сервисы KUMA на отдельных устройствах вне кластера Kubernetes или частично в кластере и вне его, вам потребуется подготовить целевые устройства KUMA к установке сервисов KUMA.

Инструкция: Подготовка устройств KUMA к установке сервисов KUMA вне кластера Kubernetes

6. **Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes (не обязательно)**

   Если вы хотите полностью установить сервисы KUMA на отдельных устройствах вне кластера Kubernetes или частично в кластере и вне его, вам потребуется подготовить файл инвентаря KUMA в формате YAML. Файл инвентаря KUMA содержит параметры для установки сервисов KUMA вне кластера Kubernetes.

   Инструкция: Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes

7. **Подготовка конфигурационного файла**

   Подготовьте конфигурационный файл в формате YAML. Конфигурационный файл содержит список целевых устройств для развертывания и набор параметров для установки компонентов Kaspersky EDR Expert.

   Если вы разворачиваете Kaspersky EDR Expert на отдельном узле, используйте конфигурационный файл, содержащий параметры установки, предназначенные для развертывания на одном узле.

   Инструкции:

   - Развертывание на нескольких узлах: параметры установки
   - Развертывание на одном узле: параметры установки

   Вы можете заполнить шаблон конфигурационного файла вручную либо вы можете использовать мастер развертывания, чтобы указать параметры установки, необходимые для развертывания Kaspersky EDR Expert, и сгенерировать конфигурационный файл.

   Инструкции: Указание параметров установки с помощью мастера развертывания.

8. **Развертывание Kaspersky EDR Expert**

   Разверните Kaspersky EDR Expert с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Kaspersky EDR Expert и другие компоненты инфраструктуры.

   Инструкции: Установка Kaspersky EDR Expert.

9. **Установка сервисов KUMA**

   Установите сервисы KUMA (коллекторы, корреляторы и хранилища).

   Сервисы KUMA можно установить полностью внутри кластера Kubernetes, полностью на отдельных узлах вне кластера или частично внутри и частично вне кластера Kubernetes.

   Инструкция: Установка сервисов KUMA вне кластера Kubernetes

   Инструкция: Установка сервисов KUMA внутри кластера Kubernetes

10. **Добавление подчиненного Сервера администрирования**

    Подчиненный Сервер администрирования требуется для дальнейшей интеграции с Endpoint Agent.

    Инструкции: Добавление подчиненного Сервера администрирования.

11. **Установка и интеграция с Endpoint Agent**

Установите Endpoint Agent в соответствии с документацией к Endpoint Agent:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Настройте интеграцию с Endpoint Agent.

12 **Установка и интеграция с Sandbox**

Установите Sandbox, настройте Sandbox и установите виртуальные машины в Sandbox.

Настройте интеграцию с Sandbox.

Развертывание на одном узле с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS

В этом разделе содержатся инструкции по развертыванию экземпляра Kaspersky EDR Expert на одном узле на стандартной виртуальной машине Ubuntu Server 24.04 LTS.

1 Аппаратные требования к узлу кластера

- 16 vCPU
- 32 ГБ оперативной памяти
- 1 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Проверка свободного места в каталогах /var, /opt и /tmp

Выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 500 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

3 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

   ```
   sudo visudo
   ```

2. Добавьте в конец файла следующую строку:

   ```
   {user} ALL=(ALL) NOPASSWD: ALL
   ```

   где `{user}` – учетная запись, используемая для развертывания.

   В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

   ```
   echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
   ```

3. Сохраните (**Ctrl+S**) и закройте файл (**Ctrl+X**).

4. Создайте SSH-ключ:

   ```
   ssh-keygen -t rsa -b 4096 -N ""
   ```

5. Скопируйте открытый ключ на целевой хост (в случае развертывания на одном узле это тот же хост, с которого вы запускаете команду):

   ```
   ssh-copy-id <IP-адрес_виртуальной_машины>
   ```

4 Установка и настройка Docker

4.1 Установка Docker

Поддерживаются версии Docker 25 и выше.

4.1.1 Установка в Ubuntu 24:

```
sudo apt update && sudo apt install docker.io
```

4.1.2 **ИЛИ** Установка с использованием официальной инструкции:

1. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

2. Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
/etc/apt/keyrings/docker.asc
```

3. Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

4. Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
plugin
```

4.2 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

5 Установка и настройка PostgreSQL

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.

- PostgreSQL 17.
- PostgreSQL 18.

1. Установите PostgreSQL:

```
sudo apt install -y postgresql-<версия>
```

где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
sudo apt install -y postgresql-16
```

Если требуемая версия PostgreSQL отсутствует в подключенном репозитории, необходимо добавить репозиторий `PostgreSQL Apt`. Подробнее см. на сайте PostgreSQL.

2. Создайте отдельного суперпользователя PostgreSQL:

```
sudo -u postgres createuser --superuser xdr
```

3. Укажите пароль пользователя:

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
```

4. Создайте для пользователя базу данных с таким же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/`<версия>`/main/postgresql.conf), где `<версия>` – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (`#`) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL:

```
sudo systemctl restart postgresql
```

6 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP.

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

7 Распаковка утилиты KDT:

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

8 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

В выводе будет текущая дата и время.

9 Создание конфигурации для запуска установки

Легенда

- `10.0.0.100` – IP-адрес хоста, на котором выполняется развертывание (`<host_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к закрытой части SSH-ключа, созданного на этапе настройки пользователя (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

9.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

```
./bin/kdt wizard -k xdr-<версия_приложения>.tar -o params.yaml
```

2. Введите количество primary_nodes (не менее 1): `1`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.100`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
6. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `0`
7. Введите `1`, если требуется балансировщик нагрузки; в противном случае нажмите **Enter**: нажмите **Enter**
8. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<your_password>@10.0.0.100:5432`
9. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`

10. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

11. Введите путь к файлу инвентаря KUMA: `/dev/null`

12. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

13. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

14. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

15. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **Enter**, чтобы пропустить этот шаг): нажмите **Enter**

16. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

17. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

18. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

9.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (singlenode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- ! → `%21`
- # → `%23`
- % → `%25`
- & → `%26`
- / → `%2F`
- : → `%3A`
- = → `%3D`
- ? → `%3F`
- @ → `%40`
- [→ `%5B`
-] → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
```

```yaml
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary-worker
    host: <host_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<ваш_пароль>@<host_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: low_resources
    source:
      value: "true"
  - name: openbao_ha_mode
    source:
      value: "false"
  - name: default_class_replica_count
    source:
      value: "1"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "ваш_пароль"
```

10 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
```

```
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 6 этой процедуры.

Развертывание на одном узле с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)

В этом разделе содержатся инструкции по развертыванию экземпляра Kaspersky EDR Expert на одном узле на стандартной виртуальной машине с операционной системой Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.2) усиленной версии ("Воронеж").

1 Аппаратные требования к узлу кластера

- 16 vCPU
- 32 ГБ оперативной памяти
- 1 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Проверка свободного места в каталогах /var, /opt и /tmp

Выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 500 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

3 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

4 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

   ```
   sudo visudo
   ```

2. Добавьте в конец файла следующую строку:

   ```
   {user} ALL=(ALL) NOPASSWD: ALL
   ```

   где `{user}` – учетная запись, используемая для развертывания.

   В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

   ```
   echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
   ```

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

4. Создайте SSH-ключ:

   ```
   ssh-keygen -t rsa -b 4096 -N ""
   ```

5. Скопируйте открытый ключ на целевой хост (в случае развертывания на одном узле это тот же хост, с которого вы запускаете команду):

   ```
   ssh-copy-id <IP-адрес_виртуальной_машины>
   ```

5 Установка и настройка Docker

5.1 Установка Docker

Поддерживаются версии Docker 25 и выше.

Выполните следующую команду:

```
sudo apt update && sudo apt install docker.io
```

5.2 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

   ```
   sudo usermod -aG docker $USER
   ```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

   ```
   newgrp docker
   ```

6 Установка PostgreSQL и настройка хоста СУБД

Хост СУБД - это экземпляр СУБД, который может быть установлен как вне кластера Kubernetes, так и совместно с кластером Kubernetes.

В связи с тем, что в репозиториях Astra Linux SE 1.8.x отсутствуют поддерживаемые версии PostgreSQL, рекомендуется использовать отдельный хост вне кластера Kubernetes с другой операционной системой, в репозиториях которой будут поддерживаемые версии PostgreSQL (например, Debian или Ubuntu).

Если вы устанавливаете экземпляр СУБД совместно с кластером Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 20 vCPU
- 40 ГБ оперативной памяти
- 2.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Если вы устанавливаете экземпляр СУБД вне кластера Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.
- PostgreSQL 17.
- PostgreSQL 18.

1. Установите PostgreSQL:

   ```
   sudo apt install -y postgresql-<версия>
   ```

   где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

   ```
   sudo apt install -y postgresql-16
   ```

2. Создайте отдельного суперпользователя PostgreSQL:

   ```
   sudo -u postgres createuser --superuser xdr
   ```

3. Укажите пароль пользователя:

   ```
   sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
   ```

4. Создайте для пользователя базу данных с таким же именем:

   ```
   sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
   ```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

   ```
   echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
   ```

   где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

   ```
   echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
   ```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/<версия>/main/postgresql.conf), где <версия> – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (#) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL:

```
sudo systemctl restart postgresql
```

8. Выполните следующие команды, чтобы настроить системное время для синхронизации с NTP-сервером:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

9. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

7 Распаковка утилиты KDT:

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

8 Отключение режима мандатного контроля целостности (МКЦ), режима замкнутой программной среды в исполняемых файлах (ЗПС) и запрета трассировки ptrace

Рекомендуется отключить запрет трассировки `ptrace`. Дополнительные сведения см. в документации Astra Linux.

Отключение режима мандатного контроля целостности (МКЦ)

Выполните команду:

```
sudo astra-mic-control status
```

Если режим мандатного контроля целостности (МКЦ) `включен`, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

Отключение режима замкнутой программной среды в исполняемых файлах (ЗПС)

```
sudo astra-digsig-control status
```

Если режим замкнутой программной среды в исполняемых файлах (ЗПС) включен, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

9 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

   ```
   sudo apt update
   sudo apt install -y systemd-timesyncd
   sudo timedatectl set-ntp true
   sudo timedatectl set-timezone Europe/Moscow
   sudo timedatectl set-local-rtc 0
   timedatectl status
   ```

   В выводе будет строка:

   ```
   System clock synchronized: yes
   ```

2. Чтобы проверить синхронизацию, выполните команду:

   ```
   date
   ```

   В выводе будет текущая дата и время.

10 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP.

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

11 Создание конфигурации для запуска установки

Легенда

- `10.0.0.100` – IP-адрес хоста, на котором выполняется развертывание (`<host_ip>`)
- `10.0.0.150` - IP-адрес хоста, на котором развернут экземпляр СУБД (`<pg_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к закрытой части SSH-ключа, созданного на этапе настройки пользователя (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

11.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

   ```
   ./bin/kdt wizard -k xdr-<версия_приложения>.tar -o params.yaml
   ```

2. Введите количество primary_nodes (не менее 1): `1`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.100`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`

6. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `0`

7. Введите `1`, если требуется балансировщик нагрузки; в противном случае нажмите **Enter**: нажмите **Enter**

8. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<your_password>@10.0.0.100:5432`

9. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`

10. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

11. Введите путь к файлу инвентаря KUMA: `/dev/null`

12. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

13. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

14. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

15. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **Enter**, чтобы пропустить этот шаг): нажмите **Enter**

16. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

17. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

18. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

11.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (singlenode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- ! → `%21`
- # → `%23`

- % → %25
- & → %26
- / → %2F
- : → %3A
- = → %3D
- ? → %3F
- @ → %40
- [→ %5B
-] → %5D

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary-worker
    host: <host_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:your_password@<pg_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: low_resources
    source:
      value: "true"
  - name: openbao_ha_mode
    source:
      value: "false"
  - name: default_class_replica_count
    source:
      value: "1"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "ваш_пароль"
```

12 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 10 этой процедуры.

Развертывание на нескольких узлах с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS

В этом разделе содержатся инструкции по развертыванию Kaspersky EDR Expert на нескольких узлах на стандартных виртуальных машинах Ubuntu Server 24.04 LTS.

1 Типовая конфигурация из четырех виртуальных машин с минимальными системными требованиями

- Управляющий узел: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 500 ГБ
- Рабочие узлы worker1, worker2 и worker3: 10 vCPU, 20 ГБ оперативной памяти, SSD* объемом 1 ТБ

* Или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

> Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Настройка хостов primary, worker1, worker2 и worker3

2.1 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

```
sudo visudo
```

2. Добавьте в конец файла следующую строку:

```
{user} ALL=(ALL) NOPASSWD: ALL
```

где `{user}` – учетная запись, используемая для развертывания.

В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

```
echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
```

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

2.2 Проверка свободного места в каталогах /var, /opt и /tmp

1. На управляющем узле выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 200 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

2. На узлах worker1–worker3 выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 700 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

2.3 Обеспечение отсутствия ошибок при синхронизации репозиториев

Выполните следующую команду:

```
sudo apt update
```

Команда не должна возвращать ошибки.

2.4 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

2.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

В выводе будет строка:

```
System clock synchronized: yes
```

2. Если команда `timedatectl` возвращает "`System clock synchronized: no`", выполните тест сетевой связности:

```
ping google.com
```

3. Если тест не пройден, в файле /etc/systemd/resolved.conf раскомментируйте строку `DNS=` и задайте в ней значение 8.8.8.8.

4. Выполните следующие команды:

```
systemctl restart systemd-resolved
apt install chrony
sudo systemctl restart chronyd
sudo systemctl enable chronyd
chronyc sources -v
chronyc tracking
sudo apt install ntpsec-ntpdate
ntpdate -q time.google.com
sudo ntpdate -u time.google.com
timedatectl status
```

В выводе будет строка:

```
System clock synchronized: yes
```

5. Чтобы проверить синхронизацию, выполните команду:

```
date
```

В выводе будет текущая дата и время.

3 Настройка устройства СУБД

Хост СУБД - это экземпляр СУБД, который может быть установлен как вне кластера Kubernetes, так и совместно с кластером Kubernetes.

Если вы устанавливаете экземпляр СУБД совместно с кластером Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 20 vCPU
- 40 ГБ оперативной памяти
- 2.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Если вы устанавливаете экземпляр СУБД вне кластера Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.

- PostgreSQL 17.
- PostgreSQL 18.

3.1 Установка и настройка PostgreSQL

1. Установите PostgreSQL:

```
sudo apt install -y postgresql-<версия>
```

где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
sudo apt install -y postgresql-16
```

Если требуемая версия PostgreSQL отсутствует в подключенном репозитории, необходимо добавить репозиторий `PostgreSQL Apt`. Подробнее см. на сайте PostgreSQL.

2. Создайте отдельного суперпользователя PostgreSQL:

```
sudo -u postgres createuser --superuser xdr
```

3. Укажите пароль пользователя:

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
```

4. Создайте для пользователя базу данных с таким же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/`<версия>`/main/postgresql.conf), где `<версия>` – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (`#`) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Если команда `timedatectl` возвращает "`System clock synchronized: no`", выполните тест сетевой связности:

```
ping google.com
```

3. Если тест не пройден, в файле /etc/systemd/resolved.conf раскомментируйте строку `DNS=` и задайте в ней значение `8`.8.8.8.

4. Выполните следующие команды:

```
systemctl restart systemd-resolved
apt install chrony
sudo systemctl restart chronyd
sudo systemctl enable chronyd
chronyc sources -v
chronyc tracking
sudo apt install ntpsec-ntpdate
ntpdate -q time.google.com
sudo ntpdate -u time.google.com
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

5. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4 Настройка устройства администратора

Устройство администратора – это устройство, с которого запускается утилита KDT. Файлы из дистрибутива, включая архив с утилитой KDT, должны находиться на хосте администратора. Это устройство может быть частью кластера Kubernetes, созданного утилитой KDT во время развертывания, или может оставаться за пределами кластера. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и OSMP. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов OSMP.

4.1 Распаковка утилиты KDT

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Установка Docker

Поддерживаются версии Docker 25 и выше.

4.2.1 Установка в Ubuntu 24:

```
sudo apt update && sudo apt install docker.io
```

4.2.2 **ИЛИ** Установка с использованием официальной инструкции:

1. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

2. Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
/etc/apt/keyrings/docker.asc
```

3. Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

4. Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
plugin
```

4.3 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

4.4 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

В выводе будет строка:

```
System clock synchronized: yes
```

2. Если команда `timedatectl` возвращает "`System clock synchronized: no`", выполните тест сетевой связности:

```
ping google.com
```

3. Если тест не пройден, в файле /etc/systemd/resolved.conf раскомментируйте строку `DNS=` и задайте в ней значение `8`.8.8.8.

4. Выполните следующие команды:

```
systemctl restart systemd-resolved
apt install chrony
sudo systemctl restart chronyd
sudo systemctl enable chronyd
chronyc sources -v
chronyc tracking
sudo apt install ntpsec-ntpdate
ntpdate -q time.google.com
sudo ntpdate -u time.google.com
timedatectl status
```

В выводе будет строка:

```
System clock synchronized: yes
```

5. Чтобы проверить синхронизацию, выполните команду:

```
date
```

В выводе будет текущая дата и время.

4.5 Проверка свободного места в директории /tmp

Выполните следующую команду:

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

Если у вас недостаточно свободного места в директории /tmp, укажите путь к другой директории:

```
export TMPDIR=<новая_директория>/tmp
```

Или добавьте место в необходимом объеме:

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

Выделив необходимое место, перезагрузите хост или повторно смонтируйте раздел.

4.6 Настройка SSH-соединения между устройством администратора и узлами primary, worker1, worker2 и worker3

1. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. Скопируйте ключ на каждый целевой хост по очереди:

```
ssh-copy-id {user}@{primary_ip}
ssh-copy-id {user}@{worker1_ip}
ssh-copy-id {user}@{worker2_ip}
ssh-copy-id {user}@{worker3_ip}
```

Где `{user}` – учетная запись пользователя для развертывания Kaspersky EDR Expert, созданная во время настройки целевого устройства.

4.7 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP (`<ingress_domain>`).

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

4.8 Создание конфигурации для запуска установки

Легенда

- `10.0.0.100` – IP-адрес управляющего узла (`<primary_ip>`)
- `10.0.0.101` – IP-адрес узла worker1 (`<worker1_ip>`)
- `10.0.0.102` – IP-адрес узла worker2 (`<worker2_ip>`)
- `10.0.0.103` – IP-адрес узла worker3 (`<worker3_ip>`)
- `10.0.0.150` – IP-адрес устройства СУБД (`<DB_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к SSH-ключу, созданному при настройке SSH-соединения на устройстве администратора (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

4.8.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

   ```
   ./bin/kdt wizard -k xdr-<версия_приложения>.tar -o params.yaml
   ```

2. Введите количество primary_nodes (не менее 1): `1`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.100`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
6. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `3`
7. Введите IPv4-адрес первого рабочего узла: `10.0.0.101`
8. Введите имя пользователя для подключения к первому рабочему узлу: `user`

9. Введите путь к SSH-ключу для подключения к первому рабочему узлу: `/home/user/.ssh/id_rsa`

10. Введите IPv4-адрес второго рабочего узла: `10.0.0.102`

11. Введите имя пользователя для подключения ко второму рабочему узлу: `user`

12. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`

13. Введите IPv4-адрес третьего рабочего узла: `10.0.0.103`

14. Введите имя пользователя для подключения к третьему рабочему узлу: `user`

15. Введите путь к SSH-ключу для подключения к третьему рабочему узлу: `/home/user/.ssh/id_rsa`

16. Введите 1, если требуется балансировщик нагрузки; в противном случае нажмите **`Enter`**: нажмите **`Enter`**

17. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<ваш_пароль>@10.0.0.150:5432`

18. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`

19. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

20. Введите путь к файлу инвентаря KUMA: `/dev/null`

21. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

22. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

23. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

24. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **`Enter`**, чтобы пропустить этот шаг): нажмите **`Enter`**

25. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

26. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

27. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

4.8.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- ! → `%21`
- # → `%23`
- % → `%25`
- & → `%26`
- / → `%2F`
- : → `%3A`
- = → `%3D`
- ? → `%3F`
- @ → `%40`
- [→ `%5B`
-] → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary
    host: <primary_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w0
    type: worker
    host: <worker1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    host: <worker2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    host: <worker3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<ваш_пароль>@<DB_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: inventory
    source:
      value: /dev/null
```

```
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "ваш_пароль"
```

5 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 4.6 этой процедуры.

Развертывание на нескольких узлах с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)

В этом разделе содержатся инструкции по развертыванию Kaspersky EDR Expert на нескольких узлах на стандартных виртуальных машинах с операционной системой Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.2) усиленной версии ("Воронеж").

1 Типовая конфигурация из четырех виртуальных машин с минимальными системными требованиями

- Управляющий узел: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 500 ГБ
- Рабочие узлы worker1, worker2 и worker3: 10 vCPU, 20 ГБ оперативной памяти, SSD* объемом 1 ТБ

* Или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

> Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Настройка хостов primary, worker1, worker2 и worker3

2.1 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

```
sudo visudo
```

2. Добавьте в конец файла следующую строку:

```
{user} ALL=(ALL) NOPASSWD: ALL
```

   где `{user}` – учетная запись, используемая для развертывания.

   В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

```
echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
```

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

2.2 Проверка свободного места в каталогах /var, /opt и /tmp

1. На управляющем узле выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2. На узлах worker1–worker4 выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 700 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2.3 Обеспечение отсутствия ошибок при синхронизации репозиториев

Выполните следующую команду:

```
sudo apt update
```

Команда не должна возвращать ошибки.

2.4 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

2.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

2.6 Отключение режима мандатного контроля целостности (МКЦ), режима замкнутой программной среды в исполняемых файлах (ЗПС) и запрета трассировки ptrace

Рекомендуется отключить запрет трассировки `ptrace`. Дополнительные сведения см. в документации Astra Linux.

Отключение режима мандатного контроля целостности (МКЦ)

Выполните команду:

```
sudo astra-mic-control status
```

Если режим мандатного контроля целостности (МКЦ) `включен`, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

Отключение режима замкнутой программной среды в исполняемых файлах (ЗПС)

```
sudo astra-digsig-control status
```

Если режим замкнутой программной среды в исполняемых файлах (ЗПС) включен, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

3 Настройка устройства СУБД

Хост СУБД - это экземпляр СУБД, который может быть установлен как вне кластера Kubernetes, так и совместно с кластером Kubernetes.

В связи с тем, что в репозиториях Astra Linux SE 1.8.x отсутствуют поддерживаемые версии PostgreSQL, рекомендуется использовать отдельный хост вне кластера Kubernetes с другой операционной системой, в репозиториях которой будут поддерживаемые версии PostgreSQL (например, Debian или Ubuntu).

Если вы устанавливаете экземпляр СУБД совместно с кластером Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 20 vCPU
- 40 ГБ оперативной памяти
- 2.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Если вы устанавливаете экземпляр СУБД вне кластера Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.
- PostgreSQL 17.
- PostgreSQL 18.

3.1 Установка и настройка PostgreSQL

1. Установите PostgreSQL:

   ```
   sudo apt install -y postgresql-<версия>
   ```

   где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

   ```
   sudo apt install -y postgresql-16
   ```

2. Создайте отдельного суперпользователя PostgreSQL:

   ```
   sudo -u postgres createuser --superuser xdr
   ```

3. Укажите пароль пользователя:

   ```
   sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
   ```

4. Создайте для пользователя базу данных с таким же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где <версия> – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/<версия>/main/postgresql.conf), где <версия> – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (#) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4 Настройка устройства администратора

Устройство администратора – это устройство, с которого запускается утилита KDT. Файлы из дистрибутива, включая архив с утилитой KDT, должны находиться на хосте администратора. Это устройство может быть частью кластера Kubernetes, созданного утилитой KDT во время развертывания, или может оставаться за пределами кластера. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и OSMP. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов OSMP.

4.1 Распаковка утилиты KDT

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Отключение режимов мандатного контроля целостности (МКЦ) и замкнутой программной среды в исполняемых файлах (ЗПС)

Рекомендуется отключить запрет трассировки `ptrace`. Дополнительные сведения см. в документации Astra Linux.

Отключение режима мандатного контроля целостности (МКЦ)

Выполните команду:

```
sudo astra-mic-control status
```

Если режим мандатного контроля целостности (МКЦ) `включен`, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

Отключение режима замкнутой программной среды в исполняемых файлах (ЗПС)

```
sudo astra-digsig-control status
```

Если режим замкнутой программной среды в исполняемых файлах (ЗПС) включен, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

4.3 Установка Docker

Поддерживаются версии Docker 25 и выше.

Выполните следующую команду:

```
sudo apt update && sudo apt install docker.io
```

4.4 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

4.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4.6 Проверка свободного места в директории /tmp

Выполните следующую команду:

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

Если у вас недостаточно свободного места в директории /tmp, укажите путь к другой директории:

```
export TMPDIR=<новая_директория>/tmp
```

Или добавьте место в необходимом объеме:

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

Выделив необходимое место, перезагрузите хост или повторно смонтируйте раздел.

4.7 Настройка SSH-соединения между устройством администратора и узлами primary, worker1, worker2 и worker3

1. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. Скопируйте ключ на каждый целевой хост по очереди:

```
ssh-copy-id {user}@{primary_ip}
ssh-copy-id {user}@{worker1_ip}
ssh-copy-id {user}@{worker2_ip}
ssh-copy-id {user}@{worker3_ip}
```

Где `{user}` – учетная запись пользователя для развертывания Kaspersky EDR Expert, созданная во время настройки целевого устройства.

4.8 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP (`<ingress_domain>`).

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

4.9 Создание конфигурации для запуска установки

Легенда

- `10.0.0.100` – IP-адрес управляющего узла (`<primary_ip>`)
- `10.0.0.101` – IP-адрес узла worker1 (`<worker1_ip>`)
- `10.0.0.102` – IP-адрес узла worker2 (`<worker2_ip>`)
- `10.0.0.103` – IP-адрес узла worker3 (`<worker3_ip>`)
- `10.0.0.150` – IP-адрес устройства СУБД (`<DB_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)

- `/home/user/.ssh/id_rsa` – путь к SSH-ключу, созданному при настройке SSH-соединения на устройстве администратора (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

4.9.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

   ```
   ./bin/kdt wizard -k xdr-<версия_приложения>.tar -o params.yaml
   ```

2. Введите количество primary_nodes (не менее 1): `1`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.100`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
6. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `3`
7. Введите IPv4-адрес первого рабочего узла: `10.0.0.101`
8. Введите имя пользователя для подключения к первому рабочему узлу: `user`
9. Введите путь к SSH-ключу для подключения к первому рабочему узлу: `/home/user/.ssh/id_rsa`
10. Введите IPv4-адрес второго рабочего узла: `10.0.0.102`
11. Введите имя пользователя для подключения ко второму рабочему узлу: `user`
12. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`
13. Введите IPv4-адрес третьего рабочего узла: `10.0.0.103`
14. Введите имя пользователя для подключения к третьему рабочему узлу: `user`
15. Введите путь к SSH-ключу для подключения к третьему рабочему узлу: `/home/user/.ssh/id_rsa`
16. Введите 1, если требуется балансировщик нагрузки; в противном случае нажмите **Enter**: нажмите **Enter**
17. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<ваш_пароль>@10.0.0.150:5432`
18. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`
19. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

20. Введите путь к файлу инвентаря KUMA: `/dev/null`

21. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

22. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

23. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

24. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **Enter**, чтобы пропустить этот шаг): нажмите **Enter**

25. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

26. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

27. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

4.9.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- ! → `%21`
- `#` → `%23`
- `%` → `%25`
- `&` → `%26`
- `/` → `%2F`
- `:` → `%3A`
- `=` → `%3D`
- `?` → `%3F`
- `@` → `%40`
- `[` → `%5B`
- `]` → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary
    host: <primary_ip>
```

```
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w0
    type: worker
    host: <worker1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    host: <worker2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    host: <worker3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:your_password@<DB_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "ваш_пароль"
```

5 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
```

```
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 4.8 этой процедуры.

Развертывание в отказоустойчивой конфигурации с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS

В этом разделе содержатся инструкции по развертыванию Kaspersky EDR Expert на нескольких узлах на стандартных виртуальных машинах Ubuntu Server 24.04 LTS.

1 Типовая конфигурация из семи виртуальных машин с минимальными системными требованиями

- Узлы primary1, primary2 и primary3: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 500 ГБ
- Узлы worker1, worker2, worker3 и worker4: 10 vCPU, 20 ГБ оперативной памяти, SSD* объемом 1 ТБ

* Или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

> Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Настройка хостов primary1, primary2, primary3, worker1, worker2, worker3 и worker4

2.1 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

```
sudo visudo
```

2. Добавьте в конец файла следующую строку:

```
{user} ALL=(ALL) NOPASSWD: ALL
```

где `{user}` – учетная запись, используемая для развертывания.

В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

```
echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
```

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

2.2 Проверка свободного места в каталогах /var, /opt и /tmp

1. На узлах primary1–primary3 выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 200 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

2. На узлах worker1–worker4 выполните следующие команды:

```
df -h /var
```

Требуется не менее 200 ГБ свободного места.

```
df -h /opt
```

Требуется не менее 700 ГБ свободного места.

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

2.3 Обеспечение отсутствия ошибок при синхронизации репозиториев

Выполните следующую команду:

```
sudo apt update
```

Команда не должна возвращать ошибки.

2.4 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

2.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

   ```
   sudo apt update
   sudo apt install -y systemd-timesyncd
   sudo timedatectl set-ntp true
   sudo timedatectl set-timezone Europe/Moscow
   sudo timedatectl set-local-rtc 0
   timedatectl status
   ```

   В выводе будет строка:

   ```
   System clock synchronized: yes
   ```

2. Чтобы проверить синхронизацию, выполните команду:

   ```
   date
   ```

   В выводе будет текущая дата и время.

3 Настройка устройства СУБД

Хост СУБД - это экземпляр СУБД, который может быть установлен как вне кластера Kubernetes, так и совместно с кластером Kubernetes.

Если вы устанавливаете экземпляр СУБД совместно с кластером Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 20 vCPU
- 40 ГБ оперативной памяти
- 2.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Если вы устанавливаете экземпляр СУБД вне кластера Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.
- PostgreSQL 17.
- PostgreSQL 18.

3.1 Установка и настройка PostgreSQL

1. Установите PostgreSQL:

   ```
   sudo apt install -y postgresql-<версия>
   ```

   где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

   ```
   sudo apt install -y postgresql-16
   ```

   Если требуемая версия PostgreSQL отсутствует в подключенном репозитории, необходимо добавить репозиторий `PostgreSQL Apt`. Подробнее см. на сайте PostgreSQL.

2. Создайте отдельного суперпользователя PostgreSQL:

   ```
   sudo -u postgres createuser --superuser xdr
   ```

3. Укажите пароль пользователя:

   ```
   sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
   ```

4. Создайте для пользователя базу данных с таким же именем:

   ```
   sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
   ```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где <версия> – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/<версия>/main/postgresql.conf), где <версия> – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (#) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4 Настройка устройства администратора

Устройство администратора – это устройство, с которого запускается утилита KDT. Файлы из дистрибутива, включая архив с утилитой KDT, должны находиться на хосте администратора. Это устройство может быть частью кластера Kubernetes, созданного утилитой KDT во время развертывания, или может оставаться за пределами кластера. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и OSMP. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов OSMP.

4.1 Распаковка утилиты KDT

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Установка Docker

Поддерживаются версии Docker 25 и выше.

4.2.1 Установка в Ubuntu 24:

```
sudo apt update && sudo apt install docker.io
```

4.2.2 **ИЛИ** Установка с использованием официальной инструкции:

1. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

2. Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
/etc/apt/keyrings/docker.asc
```

3. Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

4. Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
plugin
```

4.3 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

4.4 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4.5 Проверка свободного места в директории /tmp

Выполните следующую команду:

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

Если у вас недостаточно свободного места в директории /tmp, укажите путь к другой директории:

```
export TMPDIR=<новая_директория>/tmp
```

Или добавьте место в необходимом объеме:

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

Выделив необходимое место, перезагрузите хост или повторно смонтируйте раздел.

4.6 Настройка SSH-соединения между устройством администратора и узлами primary1, primary2, primary3, worker1, worker2, worker3 и worker4

1. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. Скопируйте ключ на каждый целевой хост по очереди:

```
ssh-copy-id {user}@{primary1_ip}
ssh-copy-id {user}@{primary2_ip}
ssh-copy-id {user}@{primary3_ip}
ssh-copy-id {user}@{worker1_ip}
ssh-copy-id {user}@{worker2_ip}
ssh-copy-id {user}@{worker3_ip}
ssh-copy-id {user}@{worker4_ip}
```

Где `{user}` – учетная запись пользователя для развертывания Kaspersky EDR Expert, созданная во время настройки целевого устройства.

4.7 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP (`<ingress_domain>`).

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

4.8 Создание конфигурации для запуска установки

Легенда

- `10.0.0.110` – IP-адрес управляющего узла (`<primary1_ip>`)
- `10.0.0.120` – IP-адрес управляющего узла (`<primary2_ip>`)
- `10.0.0.130` – IP-адрес управляющего узла (`<primary3_ip>`)
- `10.0.0.101` – IP-адрес узла worker1 (`<worker1_ip>`)
- `10.0.0.102` – IP-адрес узла worker2 (`<worker2_ip>`)
- `10.0.0.103` – IP-адрес узла worker3 (`<worker3_ip>`)
- `10.0.0.104` – IP-адрес узла worker4 (`<worker4_ip>`)

- `10.0.0.150` – IP-адрес устройства СУБД (`<DB_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к SSH-ключу, созданному при настройке SSH-соединения на устройстве администратора (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

4.8.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

   ```
   ./bin/kdt wizard -k xdr-<версия>.tar -o params.yaml
   ```

2. Введите количество primary_nodes (не менее 1): `3`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.110`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
6. Введите IPv4-адрес второго управляющего узла: `10.0.0.120`
7. Введите имя пользователя для подключения ко второму управляющему узлу: `user`
8. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`
9. Введите IPv4-адрес третьего управляющего узла: `10.0.0.130`
10. Введите имя пользователя для подключения к третьему управляющему узлу: `user`
11. Введите путь к SSH-ключу для подключения к третьему управляющему узлу: `/home/user/.ssh/id_rsa`
12. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `4`
13. Введите IPv4-адрес первого рабочего узла: `10.0.0.101`
14. Введите имя пользователя для подключения к первому рабочему узлу: `user`
15. Введите путь к SSH-ключу для подключения к первому рабочему узлу: `/home/user/.ssh/id_rsa`
16. Введите IPv4-адрес второго рабочего узла: `10.0.0.102`
17. Введите имя пользователя для подключения ко второму рабочему узлу: `user`
18. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`
19. Введите IPv4-адрес третьего рабочего узла: `10.0.0.103`

20. Введите имя пользователя для подключения к третьему рабочему узлу: `user`

21. Введите путь к SSH-ключу для подключения к третьему рабочему узлу: `/home/user/.ssh/id_rsa`

22. Введите IPv4-адрес четвертого рабочего узла: `10.0.0.104`

23. Введите имя пользователя для подключения к четвертому рабочему узлу: `user`

24. Введите путь к SSH-ключу для подключения к четвертому рабочему узлу: `/home/user/.ssh/id_rsa`

25. Введите 1, если требуется балансировщик нагрузки; в противном случае нажмите **Enter**: нажмите **Enter**

26. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<ваш_пароль>@10.0.0.150:5432`

27. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`

28. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

29. Введите путь к файлу инвентаря KUMA: `/dev/null`

30. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

31. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

32. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

33. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **Enter**, чтобы пропустить этот шаг): нажмите **Enter**

34. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

35. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

36. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

4.8.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- ! → `%21`
- # → `%23`
- % → `%25`
- & → `%26`
- / → `%2F`
- : → `%3A`
- = → `%3D`
- ? → `%3F`
- @ → `%40`
- [→ `%5B`
-] → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary
    host: <primary1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary1
    type: primary
    host: <primary2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary2
    type: primary
    host: <primary3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w0
    type: worker
    host: <worker1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    host: <worker2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    host: <worker3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w3
    type: worker
    host: <worker4_ip>
    access:
      ssh:
        user: <user_name>
```

```
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<ваш_пароль>@<DB_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "ваш_пароль"
```

5 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 4.6 этой процедуры.

Развертывание в отказоустойчивой конфигурации с помощью стандартной виртуальной машины Astra Linux Special Edition (очередное обновление 1.8.2)

В этом разделе содержатся инструкции по развертыванию Kaspersky EDR Expert на нескольких узлах на стандартных виртуальных машинах с операционной системой Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.2) усиленной версии ("Воронеж").

1 Типовая конфигурация из семи виртуальных машин с минимальными системными требованиями

- Узлы primary1, primary2 и primary3: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 500 ГБ
- Узлы worker1, worker2, worker3 и worker4: 10 vCPU, 20 ГБ оперативной памяти, SSD* объемом 1 ТБ

* Или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

> Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Настройка хостов primary1, primary2, primary3, worker1, worker2, worker3 и worker4

2.1 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

```
sudo visudo
```

2. Добавьте в конец файла следующую строку:

```
{user} ALL=(ALL) NOPASSWD: ALL
```

где `{user}` – учетная запись, используемая для развертывания.

В случае ошибки `"user is not in sudoers file"` переключитесь на пользователя с правами root и выполните следующую команду:

```
echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
```

3. Сохраните (**Ctrl+S**) и закройте файл (**Ctrl+X**).

2.2 Проверка свободного места в каталогах /var, /opt и /tmp

1. На узлах primary1–primary3 выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2. На узлах worker1–worker4 выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 700 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2.3 Обеспечение отсутствия ошибок при синхронизации репозиториев

Выполните следующую команду:

```
sudo apt update
```

Команда не должна возвращать ошибки.

2.4 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

2.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

2.6 Отключение режима мандатного контроля целостности (МКЦ), режима замкнутой программной среды в исполняемых файлах (ЗПС) и запрета трассировки ptrace

Рекомендуется отключить запрет трассировки `ptrace`. Дополнительные сведения см. в документации Astra Linux.

Отключение режима мандатного контроля целостности (МКЦ)

Выполните команду:

```
sudo astra-mic-control status
```

Если режим мандатного контроля целостности (МКЦ) `включен`, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

Отключение режима замкнутой программной среды в исполняемых файлах (ЗПС)

```
sudo astra-digsig-control status
```

Если режим замкнутой программной среды в исполняемых файлах (ЗПС) включен, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

3 Настройка устройства СУБД

Хост СУБД - это экземпляр СУБД, который может быть установлен как вне кластера Kubernetes, так и совместно с кластером Kubernetes.

В связи с тем, что в репозиториях Astra Linux SE 1.8.x отсутствуют поддерживаемые версии PostgreSQL, рекомендуется использовать отдельный хост вне кластера Kubernetes с другой операционной системой, в репозиториях которой будут поддерживаемые версии PostgreSQL (например, Debian или Ubuntu).

Если вы устанавливаете экземпляр СУБД совместно с кластером Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 20 vCPU
- 40 ГБ оперативной памяти
- 2.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Если вы устанавливаете экземпляр СУБД вне кластера Kubernetes, вы должны увеличить сайзинг целевого хоста, на котором будет установлен экземпляр СУБД, до следующего:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаются следующие версии PostgreSQL:

- PostgreSQL 15.
- PostgreSQL 16.
- PostgreSQL 17.
- PostgreSQL 18.

3.1 Установка и настройка PostgreSQL

1. Установите PostgreSQL:

   ```
   sudo apt install -y postgresql-<версия>
   ```

   где `<версия>` – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

   ```
   sudo apt install -y postgresql-16
   ```

2. Создайте отдельного суперпользователя PostgreSQL:

   ```
   sudo -u postgres createuser --superuser xdr
   ```

3. Укажите пароль пользователя:

   ```
   sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
   ```

4. Создайте для пользователя базу данных с таким же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где <версия> – поддерживаемые версии PostgreSQL. Например, для PostgreSQL 16:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/16/main/pg_hba.conf
```

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/<версия>/main/postgresql.conf), где <версия> – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (#) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4 Настройка устройства администратора

Устройство администратора – это устройство, с которого запускается утилита KDT. Файлы из дистрибутива, включая архив с утилитой KDT, должны находиться на хосте администратора. Это устройство может быть частью кластера Kubernetes, созданного утилитой KDT во время развертывания, или может оставаться за пределами кластера. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и OSMP. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов OSMP.

4.1 Распаковка утилиты KDT

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Отключение режимов мандатного контроля целостности (МКЦ) и замкнутой программной среды в исполняемых файлах (ЗПС)

Рекомендуется отключить запрет трассировки `ptrace`. Дополнительные сведения см. в документации Astra Linux.

Отключение режима мандатного контроля целостности (МКЦ)

Выполните команду:

```
sudo astra-mic-control status
```

Если режим мандатного контроля целостности (МКЦ) `включен`, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

Отключение режима замкнутой программной среды в исполняемых файлах (ЗПС)

```
sudo astra-digsig-control status
```

Если режим замкнутой программной среды в исполняемых файлах (ЗПС) включен, необходимо его отключить. Дополнительные сведения см. в документации Astra Linux.

4.3 Установка Docker

Поддерживаются версии Docker 25 и выше.

Выполните следующую команду:

```
sudo apt update && sudo apt install docker.io
```

4.4 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

4.5 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4.6 Проверка свободного места в директории /tmp

Выполните следующую команду:

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

Если у вас недостаточно свободного места в директории /tmp, укажите путь к другой директории:

```
export TMPDIR=<новая_директория>/tmp
```

Или добавьте место в необходимом объеме:

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

Выделив необходимое место, перезагрузите хост или повторно смонтируйте раздел.

4.7 Настройка SSH-соединения между устройством администратора и узлами primary1, primary2, primary3, worker1, worker2, worker3 и worker4

1. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. Скопируйте ключ на каждый целевой хост по очереди:

```
ssh-copy-id {user}@{primary1_ip}
ssh-copy-id {user}@{primary2_ip}
ssh-copy-id {user}@{primary3_ip}
ssh-copy-id {user}@{worker1_ip}
ssh-copy-id {user}@{worker2_ip}
ssh-copy-id {user}@{worker3_ip}
ssh-copy-id {user}@{worker4_ip}
```

Где `{user}` – учетная запись пользователя для развертывания Kaspersky EDR Expert, созданная во время настройки целевого устройства.

4.8 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN сервисов для подключения к сервисам OSMP (`<ingress_domain>`).

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes будет прослушивать этот IP-адрес и направлять трафик к соответствующим службам.

По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

4.9 Создание конфигурации для запуска установки

Легенда

- `10.0.0.110` – IP-адрес управляющего узла (`<primary1_ip>`)
- `10.0.0.120` – IP-адрес управляющего узла (`<primary2_ip>`)
- `10.0.0.130` – IP-адрес управляющего узла (`<primary3_ip>`)
- `10.0.0.101` – IP-адрес узла worker1 (`<worker1_ip>`)
- `10.0.0.102` – IP-адрес узла worker2 (`<worker2_ip>`)
- `10.0.0.103` – IP-адрес узла worker3 (`<worker3_ip>`)
- `10.0.0.104` – IP-адрес узла worker4 (`<worker4_ip>`)

- `10.0.0.150` – IP-адрес устройства СУБД (`<DB_ip>`)
- `10.0.0.200` – IP-адрес, используемый для записи с подстановкой A на этапе настройки DNS (`<ingress_ip>`)
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к SSH-ключу, созданному при настройке SSH-соединения на устройстве администратора (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<ingress_domain>`)

4.9.1 Указание параметров установки с помощью мастера настройки

1. Выполните следующую команду, чтобы запустить мастер настройки:

   ```
   ./bin/kdt wizard -k xdr-<версия>.tar -o params.yaml
   ```

2. Введите количество primary_nodes (не менее 1): `3`
3. Введите IPv4-адрес первого управляющего узла: `10.0.0.110`
4. Введите имя пользователя для подключения к первому управляющему узлу: `user`
5. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
6. Введите IPv4-адрес второго управляющего узла: `10.0.0.120`
7. Введите имя пользователя для подключения ко второму управляющему узлу: `user`
8. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`
9. Введите IPv4-адрес третьего управляющего узла: `10.0.0.130`
10. Введите имя пользователя для подключения к третьему управляющему узлу: `user`
11. Введите путь к SSH-ключу для подключения к третьему управляющему узлу: `/home/user/.ssh/id_rsa`
12. Введите количество worker_nodes (0 – развертывание на одном узле, 3 и более – развертывание на нескольких узлах): `4`
13. Введите IPv4-адрес первого рабочего узла: `10.0.0.101`
14. Введите имя пользователя для подключения к первому рабочему узлу: `user`
15. Введите путь к SSH-ключу для подключения к первому рабочему узлу: `/home/user/.ssh/id_rsa`
16. Введите IPv4-адрес второго рабочего узла: `10.0.0.102`
17. Введите имя пользователя для подключения ко второму рабочему узлу: `user`
18. Введите путь к SSH-ключу для подключения ко второму управляющему узлу: `/home/user/.ssh/id_rsa`
19. Введите IPv4-адрес третьего рабочего узла: `10.0.0.103`

20. Введите имя пользователя для подключения к третьему рабочему узлу: `user`

21. Введите путь к SSH-ключу для подключения к третьему рабочему узлу: `/home/user/.ssh/id_rsa`

22. Введите IPv4-адрес четвертого рабочего узла: `10.0.0.104`

23. Введите имя пользователя для подключения к четвертому рабочему узлу: `user`

24. Введите путь к SSH-ключу для подключения к четвертому рабочему узлу: `/home/user/.ssh/id_rsa`

25. Введите 1, если требуется балансировщик нагрузки; в противном случае нажмите **Enter**: нажмите **Enter**

26. Введите строку подключения для доступа к СУБД: postgres://<dbms_username>:<password>@<fqdn>:<port>: `postgres://xdr:<ваш_пароль>@10.0.0.150:5432`

27. Требуется ввести IP-адрес шлюза кластера Kubernetes следующим образом: <ip_address>. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Введите IP-адрес: `10.0.0.200`

28. Требуется создать учетную запись пользователя Kaspersky EDR Expert. Введите пароль учетной записи пользователя Kaspersky EDR Expert, которая будет создана KDT во время установки. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы. Введите пароль: `ваш_пароль`

29. Введите путь к файлу инвентаря KUMA: `/dev/null`

30. Введите путь к SSH-ключу, который используется для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`

31. Введите путь к файлу лицензионного ключа KUMA: `/dev/null`

32. Требуется доменное имя для публичных служб Kaspersky EDR Expert. Это доменное имя будет включено в доменные имена служб Kaspersky EDR Expert. Например, console.<domain name>. Введите доменное имя: `xdr.mydomain.com`

33. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов Kaspersky EDR Expert (если вы хотите использовать самоподписанный сертификат, нажмите **Enter**, чтобы пропустить этот шаг): нажмите **Enter**

34. Введите "Y", если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`

35. Введите имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Имя пользователя не может содержать менее 1 и более 30 символов. Имя пользователя должно начинаться с буквы и может содержать строчные буквы (от "a" до "z"), цифры (от "0" до "9") и специальные символы (_ -.): `xdr`

36. Введите пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana. Пароль не может содержать менее 8 и более 256 символов. Пароль должен содержать прописные и строчные буквы, цифры и специальные символы: `ваш_пароль`

4.9.2 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- `!` → `%21`
- `#` → `%23`
- `%` → `%25`
- `&` → `%26`
- `/` → `%2F`
- `:` → `%3A`
- `=` → `%3D`
- `?` → `%3F`
- `@` → `%40`
- `[` → `%5B`
- `]` → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary
    host: <primary1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary1
    type: primary
    host: <primary2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary2
    type: primary
    host: <primary3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w0
    type: worker
    host: <worker1_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    host: <worker2_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    host: <worker3_ip>
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w3
    type: worker
    host: <worker4_ip>
    access:
      ssh:
        user: <user_name>
```

```
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:your_password@<DB_ip>:5432
  - name: ingress_ip
    source:
      value: <ingress_ip>
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "ваш_пароль"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<ingress_domain>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "your_password"
```

5 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<ingress_domain>
```

Где `<ingress_domain>` – FQDN, указанное на шаге 4.8 этой процедуры.

Руководство по усилению защиты

Руководство по усилению защиты адресовано специалистам, которые осуществляют развертывание и администрирование Kaspersky EDR Expert, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky EDR Expert.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky EDR Expert и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- подготовка инфраструктуры для развертывания Kaspersky EDR Expert;
- настройка безопасного подключения к Kaspersky EDR Expert;
- настройка учетных записей для доступа к Kaspersky EDR Expert;
- управление защитой Kaspersky EDR Expert;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- передача информации в сторонние системы.

Перед тем как приступить к развертыванию Kaspersky EDR Expert, рекомендуется прочитать Руководство по усилению защиты.

Управление инфраструктурой Kaspersky EDR Expert

В этой статье описан общий принцип использования минимально необходимого количества приложений для работы операционной системы и Kaspersky EDR Expert. Также в этой статье описан принцип минимальных привилегий, который сводится к концепции нулевого доверия.

Управление учетными записями операционной системы

Для работы с кластером Kubernetes с помощью KDT рекомендуется создать отдельного пользователя с минимальными правами. Оптимальным способом является реализация управления учетными записями пользователей операционной системы с помощью LDAP с возможностью отзыва прав пользователей через LDAP. Информацию о конкретной реализации отзыва прав и блокировки пользователей см. в руководстве пользователя/администратора в вашем решении LDAP. Рекомендуется использовать пароль длиной не менее 18 символов или парольную фразу, содержащую не менее 4 слов с любыми разделителями, для аутентификации пользователя. Также можно использовать физические средства аутентификации (например, токен).

Дополнительные сведения см. в документации к ПО OpenLDAP.

Пример

Дистрибутив	Команда создания пользователя	Минимальный набор групп/прав
Ubuntu / Debian / Astra / Atlant	`useradd "$1" --shell /bin/bash --create-home --password "$(openssl passwd -1 "$2")"`	`usermod -aG sudo,root "$1"` Добавление в группу `sudo` позволяет пользователю выполнять команду `sudo` без пароля.

Также рекомендуется защищать корневую директорию документов пользователя и все вложенные директории таким образом, чтобы только пользователь имел к ним доступ. Другие пользователи и группа пользователей не должны иметь прав на корневую директорию документов.

Пример

В этом примере у пользователя `example_user` есть директория для документов `~/Documents`. По умолчанию (если пользователь создается с помощью команд `useradd или adduser` и `umask 022`) директории создаются с правами `755`. Чтобы гарантировать, что только этот пользователь имеет доступ к корневой директории и всем вложенным директории, `umask` изменяется на `077`, а также явным образом устанавливаются права доступа `700`. Ниже приведен пример команд, с помощью которых можно проверить, правильно ли заданы права (доступ только у владельца).

Чтобы вывести права доступа, владельца и группу директории:
`stat -c "%A %U %G" /home/example_user/Documents`
Ожидаемый вывод команды, если права доступа настроены правильно:
`drwx------ example_user example_user`
Если права доступа не соответствуют требованиям, установите права доступа `700` для корневой директории и всех вложенных директорий:
`chmod -R 700 /home/example_user/Documents`
Убедитесь, что владельцем является правильный пользователь:
`chown -R example_user:example_user /home/example_user/Documents`

Рекомендуется не предоставлять права на запуск для директорий .ssh, .kube, .config и .kdt, а также для всех файлов, содержащихся в этих директориях в корневой директории документов пользователя.

Пример

Показать права доступа для наиболее чувствительных директорий – показать режим, владельца и путь для каждой из указанных директорий:

```
find ~/Documents -type d \( -name .ssh -o -name .kube -o -name .config -o -name .kdt \) \

-exec stat -c "%A %U %G %n" {} \;
```

Ожидаемый вывод команды:

```
drwx------ example_user example_user /home/example_user/Documents/.ssh

drwx------ example_user example_user /home/example_user/Documents/.kube

drwx------ example_user example_user /home/example_user/Documents/.config

drwx------ example_user example_user /home/example_user/Documents/.kdt
```

`drwx------` представляет права доступа `700`: чтение, запись и выполнение только для владельца (в случае каталогов "выполнение" – это разрешение на вход в каталог, но не на запуск исполняемых файлов).

Если обнаружены лишние биты выполнения, удалите их из файлов:

```
find ~/Documents -type f \( -path "*/.ssh/*" -o -path "*/.kube/*" -o -path "*/.config/*"
-o -path "*/.kdt/*" \) -exec chmod a-x {} \;
```

Если требуется, установите более строгие права (например, `600`):

```
find ~/Documents -type f \( -path "*/.ssh/*" -o -path "*/.kube/*" -o -path "*/.config/*"
-o -path "*/.kdt/*" \) -exec chmod 600 {} \;
```

Управление пакетами операционной системы

Рекомендуется использовать минимальный набор приложений, необходимый для работы KDT и Kaspersky EDR Expert. Например, вам не нужно использовать графический пользовательский интерфейс для работы в кластере Kubernetes, поэтому не рекомендуется устанавливать графические пакеты. Если пакеты установлены, рекомендуется удалить эти пакеты, включая графические серверы, такие как Xorg или Wayland.

Рекомендуется регулярно устанавливать обновления безопасности для системного программного обеспечения и ядра Linux. Также рекомендуется включить автоматическое обновление следующим образом:

- Для операционных систем с диспетчером пакетов apt:

  /etc/apt/apt.conf.d/50unattended-upgrades

  ```
  Unattended-Upgrade::Allowed-Origins {
      "${distro_id}:${distro_codename}-security";

      "${distro_id}ESMApps:${distro_codename}-apps-security";
      "${distro_id}ESM:${distro_codename}-infra-security";
  };
  ```

- Для операционных систем с диспетчером пакетов rpm, dnf и yum:

  /etc/dnf/automatic.conf

  ```
  [commands]
  #  Какое обновление выполнить:
  # default                            = все доступные обновления
  # security                           = только обновления безопасности
  upgrade_type = default

  # Следует ли скачивать обновления, когда они будут доступны,
  # dnf-automatic.timer. notifyonly.timer, download.timer и
  # install.timer отменяют этот параметр.
  download_updates = yes

  # Следует ли применять обновления, когда они будут доступны,
  # dnf-automatic.timer. notifyonly.timer, download.timer и
  # install.timer отменяют этот параметр.
  apply_updates = no
  ```

Параметры безопасности операционной системы

Параметры безопасности ядра Linux можно включить в файле `/etc/sysctl.conf` или с помощью команды `sysctl`. Рекомендуемые параметры безопасности ядра Linux перечислены во фрагменте файла `/etc/sysctl.conf`:

/etc/sysctl.conf

```
# Выключить execshield
kernel.randomize_va_space=2
# Включить защиту от IP-спуфинга
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
# Игнорировать широковещательные сетевые запросы
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_responses=1
# Включить ведение журнала событий сетевых спуфинговых пакетов
net.ipv4.conf.all.log_martians=1
# Скрыть указатели ядра
kernel.kptr_restrict=1
# Ограничить доступ к журналам событий ядра
kernel.dmesg_restrict = 1
# Запретить профилирование ядра для непривилегированных пользователей
kernel.perf_event_paranoid=3
# Увеличение бит энтропии ASLR
vm.mmap_rnd_bits=32
vm.mmap_rnd_compat_bits=16
```

Рекомендуется ограничить доступ к PID. Это уменьшит вероятность того, что один пользователь будет отслеживать процессы другого пользователя. Вы можете ограничить доступ к PID при монтировании файловой системы `/proc`, например, добавив следующую строку в файл `/etc/fstab`:

```
proc /proc proc nosuid,nodev,noexec,hidepid=2,gid=proc 0 0
```

Если процессы операционной системы управляются с помощью системы `systemd`, служба `systemd-logind` по-прежнему может контролировать процессы других пользователей. Для корректной работы пользовательских сеансов в системе `systemd` необходимо создать файл `/etc/systemd/system/systemd-logind.service.d/hidepid.conf` и добавить в него следующие строки:

```
[Service]
SupplementaryGroups=proc
```

> Так как в некоторых системах может не быть группы `proc`, рекомендуется добавить группу `proc` заранее.

С помощью команды `systemctl mask ctrl-alt-del.target` рекомендуется выключить комбинацию клавиш **`Ctrl`**+**`Alt`**+**`Del`**, чтобы предотвратить неожиданную перезагрузку операционной системы.

Рекомендуется запретить аутентификацию привилегированных пользователей (пользователей root) для установки удаленного подключения пользователя.

Пример

Ниже приведен набор команд, которые одновременно предотвращают вход пользователя root по сети и исключают его из аутентификации LDAP.

```
# 1. SSH

sudo sed -i 's/^#\?PermitRootLogin .*/PermitRootLogin no/' /etc/ssh/sshd_config

sudo systemctl restart sshd

# 2. Local account

sudo passwd -l root

sudo usermod -s /usr/sbin/nologin root

# 3. Пример привязки LDAP; путь к файлу может отличаться

LDAP_CONF="/etc/ksc/ldap_connection.json"

if [ -f "$LDAP_CONF" ]; then

sudo jq '.ldap.bindDn = "cn=admin,dc=example,dc=com"' "$LDAP_CONF" | sudo tee
"$LDAP_CONF" > /dev/null

sudo systemctl restart ksc-orchestrator

fi

# 4. sudo без NOPASSWD

sudo sed -i '/^root.*NOPASSWD/d' /etc/sudoers
```

Рекомендуется использовать сетевой экран для ограничения сетевой активности. Об используемых портах и протоколах см. в разделе Порты, используемые Kaspersky EDR Expert.

Пример

Действие	ufw (Ubuntu/Debian)	firewalld (RHEL/CentOS)	iptables
Проверка статуса	ufw status	firewall-cmd --list-all	iptables -L -n
Проверка порта	ss -tuln | grep 443	ss -tuln | grep 443	ss -tuln | grep 443
Внешний аудит	nc -zv IP 443	nc -zv IP 443	nc -zv IP 443
Открытие порта	ufw allow 443/tcp	firewall-cmd --add-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j ACCEPT
Закрытие порта	ufw deny 443/tcp	firewall-cmd --remove-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j DROP
Сохранение правил	Auto	Auto	iptables-save > /etc/iptables/rules.v4

Рекомендуется включить `auditd`, чтобы упростить расследование инцидентов безопасности. О включении перенаправления телеметрии см. в разделе Настройка получения событий Auditd.

Рекомендуется регулярно создавать резервные копии следующих конфигураций и директорий данных:

- Устройство администратора: `~/kdt`
- Целевое устройство: `/etc/k0s/`, `/var/lib/k0s`

Также рекомендуется зашифровать эти резервные копии.

Руководства по усилению защиты для различных операционных систем и СУБД

Если вам нужно настроить параметры безопасности вашей операционной системы и программного обеспечения, вы можете использовать рекомендации, предоставленные Center for Internet Security (CIS).

Если вы используете операционную систему Astra Linux, обратитесь к рекомендациям по безопасности, которые можно применить к вашей версии Astra Linux.

Если вам необходимо настроить параметры безопасности PostgreSQL, воспользуйтесь рекомендациями по администрированию сервера из официальной документации PostgreSQL.

Безопасность соединения

Строгие параметры TLS

Рекомендуется использовать протокол TLS версии 1.2 или выше и ограничить или запретить использование небезопасных алгоритмов шифрования.

Вы можете настроить протоколы шифрования (TLS), используемые Сервером администрирования. При этом учитывайте, что на момент выпуска определенной версии Kaspersky EDR Expert параметры протокола шифрования по умолчанию настроены так, чтобы обеспечить безопасную передачу данных.

Ограничение доступа к базе данных Kaspersky EDR Expert

Рекомендуется ограничить доступ к базе данных Kaspersky EDR Expert. Например, разрешить доступ только с устройств, на которых установлен Kaspersky EDR Expert. Это позволит снизить вероятность взлома базы данных Kaspersky EDR Expert через известные уязвимости.

Вы можете настроить параметры в соответствии с руководством по эксплуатации используемой базы данных, а также предусмотреть закрытые порты на сетевых экранах.

Учетные записи и авторизация

Использование двухэтапной проверки Kaspersky EDR Expert

Kaspersky EDR Expert предоставляет пользователям **двухфакторную аутентификацию** на основе стандарта RFC 6238 (TOTP; Time-Based One-Time Password Algorithm – алгоритм одноразового пароля на основе времени).

Если для вашей учетной записи включена двухфакторная аутентификация, каждый раз при входе в Kaspersky EDR Expert с помощью браузера, вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение для аутентификации на своем компьютере или мобильном устройстве.

Существуют как программные, так и аппаратные аутентификаторы (токены), поддерживающие стандарт RFC 6238. Например, к программным аутентификаторам относятся Google Authenticator, Microsoft Authenticator, FreeOTP.

Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Kaspersky EDR Expert. Например, вы можете установить приложение для аутентификации на мобильном устройстве.

Использование двухфакторной аутентификации операционной системы

Рекомендуется использовать многофакторную аутентификацию (MFA) на устройствах с развернутым Kaspersky EDR Expert с помощью токена, смарт-карты или другим способом (если это возможно).

Запрет на сохранение пароля администратора

При работе с Kaspersky EDR Expert через браузер не рекомендуется сохранять пароль администратора в браузере на устройстве пользователя.

Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Kaspersky EDR Expert должен соответствовать следующим требованиям:

- Длина пароля должна быть от 10 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

По умолчанию максимальное количество попыток ввода пароля равно 3. Это число фиксировано и не может быть изменено.

Пользователь может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

Ограничение назначения роли Главного администратора

Пользователю назначается роль Главного администратора в списке контроля доступа (ACL) Kaspersky EDR Expert. Не рекомендуется назначать роль Главного администратора большому количеству пользователей.

Настройка прав доступа к функциям приложения

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Kaspersky EDR Expert.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты устройства с Kaspersky EDR Expert и удаленной установкой стороннего программного обеспечения:

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

  Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с OSMP при возникновении события.

Отдельная учетная запись для удаленной установки приложений

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей, кроме "Главного администратора" или иной специализированной учетной записи.

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль или разрешения отдельной учетной записи.

Регулярный аудит всех пользователей и их действий

Рекомендуется проводить регулярный аудит всех пользователей на устройстве, где развернуто приложение Kaspersky EDR Expert. Это позволит реагировать на некоторые типы угроз безопасности, связанные с возможной компрометацией устройства.

Также вы можете отслеживать действия пользователей, такие как подключение к Серверу администрирования и отключение от него, подключение к Серверу администрирования с ошибкой и изменение объектов (для объектов, поддерживающих управление версиями).

Управление защитой Kaspersky EDR Expert

Выбор программного обеспечения защиты Kaspersky EDR Expert

В зависимости от типа развертывания Kaspersky EDR Expert и общей стратегии защиты выберите приложение для защиты устройств с развернутым Kaspersky EDR Expert и устройства администратора.

Если вы разворачиваете Kaspersky EDR Expert на выделенных устройствах, рекомендуется выбрать приложение Kaspersky Endpoint Security для защиты устройств с развернутым Kaspersky EDR Expert и устройства администратора. Это позволит применить все имеющиеся технологии для защиты этих устройств, в том числе модули поведенческого анализа.

Если Kaspersky EDR Expert разворачивается на устройствах, которые уже существуют в инфраструктуре и ранее использовались для выполнения других задач, рекомендуются следующие приложения защиты:

- Kaspersky Industrial CyberSecurity for Nodes. Это приложение рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это приложение, имеющее сертификаты совместимости с различными производителями промышленного программного обеспечения.

- Рекомендованные приложения безопасности. Если Kaspersky EDR Expert развернут на устройствах с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных приложений (возможно, уже существуют рекомендации по выбору приложения защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

Модули защиты

Если отсутствуют особые рекомендации от производителя стороннего программного обеспечения, установленного на тех же устройствах, что и Kaspersky EDR Expert, рекомендуется активировать и настроить все доступные модули защиты (после проверки их работы в течение определенного времени).

Настройка сетевого экрана устройств с Kaspersky EDR Expert

На устройствах с развернутым Kaspersky EDR Expert рекомендуется настроить сетевой экран, чтобы ограничить количество устройств, с которых администраторы могут подключаться к Kaspersky EDR Expert через браузер.

По умолчанию

Kaspersky EDR Expert использует порт 443 для входа в систему через браузер. Рекомендуется ограничить число устройств, с которых Kaspersky EDR Expert может управляться по этим портам.

Управление защитой клиентских устройств

Ограничение добавления лицензионных ключей в инсталляционные пакеты

Инсталляционные пакеты можно публиковать с помощью Веб-сервера, входящего в состав Kaspersky EDR Expert. Если вы добавите лицензионный ключ в инсталляционный пакет, опубликованный на Веб-сервере, лицензионный ключ будет доступен для чтения всем пользователям.

Для того чтобы избежать компрометации лицензионного ключа, не рекомендуется добавлять лицензионные ключи в инсталляционные пакеты.

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства, выполнять развертывание с помощью задачи *Добавление лицензионного ключа* для управляемого приложения, и добавлять код активации или файл ключа на устройства вручную.

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования.

Требования безопасности к устройствам с точками распространения и шлюзам соединений

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Kaspersky EDR Expert, на клиентские устройства в группе.
- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" на клиентские устройства.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Kaspersky EDR Expert.

Размещение точек распространения в сети организации используется для следующих задач:

- снижение нагрузки на Kaspersky EDR Expert;
- оптимизация трафика;
- предоставление Kaspersky EDR Expert доступа к устройствам в труднодоступных частях сети.

С учетом доступных возможностей рекомендуется защитить, в том числе физически, устройства, выполняющие роль точек распространения, от любого типа несанкционированного доступа.

Ограничение автоматического назначения точек распространения

Для упрощения администрирования и сохранения работоспособности сети рекомендуется воспользоваться автоматическим назначением точек распространения. Однако в промышленных и небольших сетях рекомендуется избегать автоматического назначения точек распространения, так как на точки распространения могут быть, например, переданы конфиденциальные сведения учетных записей, используемых для работы задач принудительной удаленной установки средствами операционной системы.

В промышленных и небольших сетях вы можете назначить точки распространения вручную.

При необходимости вы также можете просмотреть Отчет о работе точек распространения.

Передача событий в сторонние системы

В этом разделе описаны особенности передачи проблем безопасности, обнаруженных на клиентских устройствах, в системы сторонних производителей.

Мониторинг и отчеты

Для своевременного реагирования на проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов.

Экспорт событий в SIEM-системы

Для максимально быстрого выявления проблем безопасности до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему.

Уведомление по электронной почте о событиях аудита

Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях.

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.

Настройка защиты управляемых приложений

Политики управляемых приложений

Рекомендуется создать политику для каждого вида используемого приложения и всех компонентов Kaspersky EDR Expert (Агент администрирования, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent и другие). Эта групповая политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

Установка пароля на выключение защиты и удаление приложения

Настоятельно рекомендуется включить защиту паролем, чтобы злоумышленники не смогли выключить или удалить приложения безопасности "Лаборатории Касперского". На платформах, где поддерживается защита паролем, вы можете установить пароль, например, для Kaspersky Endpoint Security, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать соответствующие параметры, закрыв их "замком".

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Kaspersky EDR Expert рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN. При обновлении Kaspersky EDR Expert вы также можете принять обновленное Положение о KSN. Если использование облачных служб запрещено законодательством или иными нормативными актами, вы можете не включать KSN.

Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу, периодически запускающую полную проверку устройств.

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с контроллерами доменов и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и применяемые к этой группе политики по умолчанию.

Схемы развертывания

Существует два варианта развертывания Kaspersky EDR Expert (включая функциональность Kaspersky Endpoint Detection and Response): на нескольких узлах или на одном узле кластера Kubernetes. Прежде чем начать, рекомендуется ознакомиться с доступными схемами развертывания и выбрать ту, которая лучше всего соответствует требованиям вашей организации. Также рекомендуется ознакомиться с Руководством по масштабированию, в котором изложены требования к оборудованию и приведены рекомендуемые варианты развертывания в зависимости от количества устройств в организации.

В зависимости от выбранного варианта развертывания для правильной работы Kaspersky EDR Expert могут потребоваться следующие устройства:

- **Устройство администратора**

  Устройство администратора – это физическая или виртуальная машина, которая используется для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Поскольку KDT работает на устройстве администратора, это устройство должно соответствовать требованиям KDT.

  Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert. В этом случае устройство должно соответствовать требованиям для целевых устройств.

- **Целевые устройства**

  Целевые устройства – это физические или виртуальные машины, на которые устанавливается Kaspersky EDR Expert. Используются следующие целевые устройства:

  - Целевые устройства для установки компонентов Kaspersky EDR Expert внутри кластера.

    Устройства, входящие в кластер Kubernetes, между которыми распределяется рабочая нагрузка. Целевые устройства должны соответствовать требованиям для выбранного варианта развертывания (развертывание на нескольких узлах или развертывание на одном узле).

    Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера, на отдельных устройствах вне кластера или частично в кластере Kubernetes и вне его. В этом случае устройства должны соответствовать требованиям к оборудованию, программному обеспечению и требованиям установки, необходимым для установки сервисов KUMA.

    Вы можете использовать одно из целевых устройств в качестве устройства администратора для выполнения развертывания Kaspersky EDR Expert. В этом случае это устройство также должно соответствовать требованиям для KDT.

  - Целевые устройства KUMA для установки сервисов KUMA (не обязательно).

    Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены на целевых устройствах вне кластера. Количество целевых устройств KUMA зависит от количества событий, которые приложение Kaspersky EDR Expert должно обработать.

    Целевые устройства KUMA должны соответствовать требованиям к оборудованию, программному обеспечению и требованиям установки, необходимым для установки сервисов KUMA.

- **Устройство СУБД (только при развертывании на нескольких узлах)**

  Устройством для установки СУБД является отдельный сервер, расположенный вне кластера Kubernetes. Это устройство должно соответствовать требованиям для узла базы данных.

Развертывание на нескольких узлах.

При развертывании на нескольких узлах компоненты Kaspersky EDR Expert устанавливаются на нескольких рабочих узлах в кластере Kubernetes. При выходе из строя одного из узлов кластер может восстановить работу компонента на другом узле.

В этой конфигурации вам понадобится минимум пять устройств:

- Одно устройство для СУБД.
- Четыре целевых устройства для кластера Kubernetes и компонентов Kaspersky EDR Expert.
  - Одно устройство, выполняющее роль как устройства администратора, так и целевого устройства.
  - Три целевых устройства.

  Если планируется использовать устройство администратора, не входящее в кластер, необходимо выделить для развертывания одно дополнительное устройство.

  Для установки сервисов KUMA вне кластера необходимо выделить как минимум одно дополнительное целевое устройство для KUMA.

Развертывание на одном узле

При развертывании на одном узле все компоненты Kaspersky EDR Expert устанавливаются на одном узле кластера Kubernetes. Этот вариант подходит для решений, требующих небольшого количества вычислительных ресурсов.

В этой конфигурации потребуется хотя бы одно устройство для установки кластера Kubernetes, компонентов Kaspersky EDR Expert и СУБД. Это устройство выполняет функции как устройства администратора, так и целевого устройства. Если желательно использовать устройство администратора, не входящее в кластер, необходимо выделить для развертывания одно дополнительное устройство.

Если требуется установить сервисы KUMA вне кластера, необходимо выделить как минимум один дополнительное целевое устройство для KUMA.

В этой конфигурации отдельный узел для СУБД не требуется. Однако СУБД необходимо вручную установить на целевое устройство перед развертыванием Kaspersky EDR Expert.

Развертывание иерархии отдельных узлов

При иерархическом развертывании используется несколько одиночных узлов. После развертывания всех одиночных узлов один из таких узлов выбирается в качестве родительского экземпляра. Как правило, родительским экземпляром становится самый мощный узел по данным расчетов. Затем остальные узлы подключаются к родительскому экземпляру.

За помощью в расчете ресурсов, необходимых для развертывания, обратитесь в Службу технической поддержки.

Схема развертывания на одном узле

На рисунке ниже приведена схема развертывания приложения Kaspersky EDR Expert на одном узле.

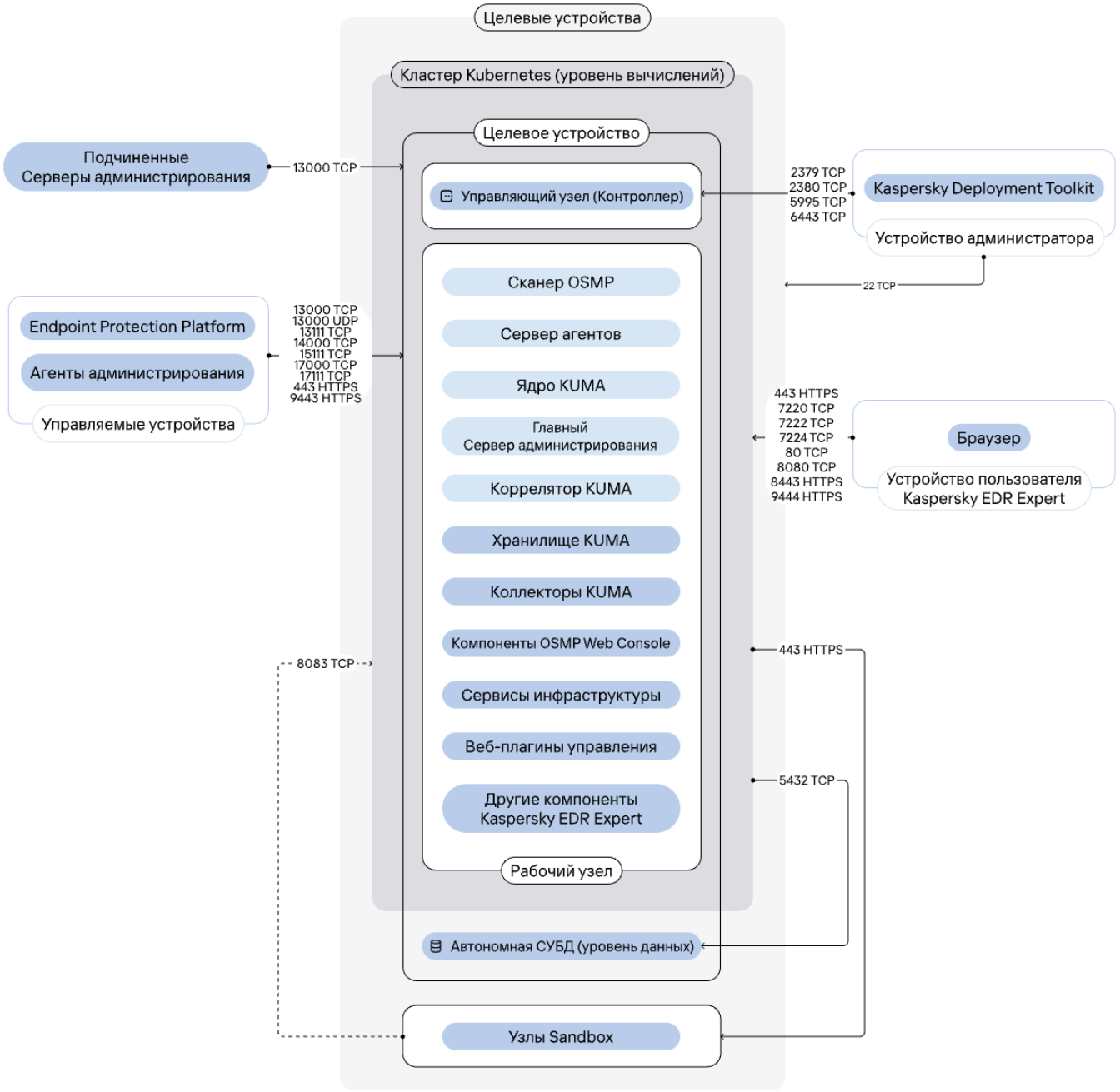


Схема развертывания Kaspersky EDR Expert на одном узле

Схема развертывания Kaspersky EDR Expert на одном узле включает следующие основные компоненты:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit (KDT) для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Этот хост может быть включен в кластер Kubernetes, созданный KDT во время развертывания, или может оставаться отдельным.

- **Сервер агентов**. Этот компонент отвечает за взаимодействие между OSMP и агентами Endpoint Agent.

- **Кластер Kubernetes**. При развертывании на одном узле кластер Kubernetes состоит из одного хоста, которое действует как узел контроллера (далее также управляющий узел во время процедуры развертывания) и как рабочий узел.

- **Автономная СУБД**. Система управления базами данных (СУБД) необходима для корректной работы компонентов Kaspersky EDR Expert. Администратор устанавливает СУБД на том же физическом хосте, что и рабочий узел Kubernetes. СУБД нельзя разворачивать в кластер Kubernetes – он действует как независимый сервис, который управляется независимо от Orchestration.

- **Ядро KUMA**. Центральный компонент SIEM (KUMA), на основе которого строятся все остальные сервисы и компоненты.

- **Коллектор KUMA**. Компонент SIEM (KUMA), который получает сообщения из источников событий, обрабатывает их и передает в хранилище KUMA и коррелятор KUMA.

- **Коррелятор KUMA**. Компонент SIEM (KUMA), анализирующий нормализованные события.

- **Хранилище KUMA**. Компонент SIEM (KUMA), используемый для хранения нормализованных событий, что позволяет обеспечивать непрерывный и эффективный доступ для аналитической обработки.

- **OSMP Scanner**. Компонент, который выполняет проверку файлов с помощью Anti-Malware Engine, YARA и Sandbox, отправляет их на анализ и формирует отчеты.

- **Узлы Sandbox**. Узел Sandbox, который может включать в себя один или несколько серверов, на которых работают компоненты Sandbox, и предоставляет выделенные вычислительные ресурсы, на которых размещаются изолированная среда выполнения и поддерживающие службы. Этот узел анализируют файлы, ссылки, URL и другие объекты, попадающие в защищаемую систему. Узлы Sandbox работают независимо от кластера Kubernetes.

  Количество серверов Sandbox может варьироваться в зависимости от требований к загрузке.

- **Веб-плагин управления**. Компонент, который используется для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP.

- **Устройство пользователя с Kaspersky EDR Expert**. Пользовательское устройство, которое используется для входа в Консоль OSMP.

- **Подчиненные Серверы администрирования** (необязательно). Эти серверы используются для создания иерархии Серверов.

- **Управляемые устройства**. Клиентские устройства защищены Kaspersky EDR Expert. На каждом управляемом устройстве установлен Агент администрирования и EPP-приложение.

- **Инфраструктурные сервисы и другие компоненты Kaspersky EDR Expert**. Решение также включает в себя дополнительные компоненты, которые обеспечивают централизованное управление активами, обмен данными, построение иерархии, аутентификацию и авторизацию, а также ряд других функций, таких как аудит действий, управление политиками безопасности и распространение обновлений.

Порты

Схема развертывания не включает все порты, необходимые для успешной установки и работы. Полный список портов приведен в разделе Порты, используемые Kaspersky EDR Expert.

Развертывание на нескольких узлах: схема профиля на четырех узлах

Развертывание профиля на четырех узлах предназначен для сред с ограниченными аппаратными ресурсами и для поддержания инфраструктурного соответствия предыдущим развертываниям. Архитектура из четырех узлов обеспечивает баланс между требованиями к аппаратному обеспечению и необходимостью выполнения всех основных функциональных задач. Такое развертывание минимизирует затраты на инфраструктуру, сохраняя полную совместимость с целевыми службами. На рисунке ниже показана схема развертывания Kaspersky EDR Expert на нескольких узлах.

Для установок с высокой вычислительной нагрузкой рекомендуется развертывание на шести узлах.

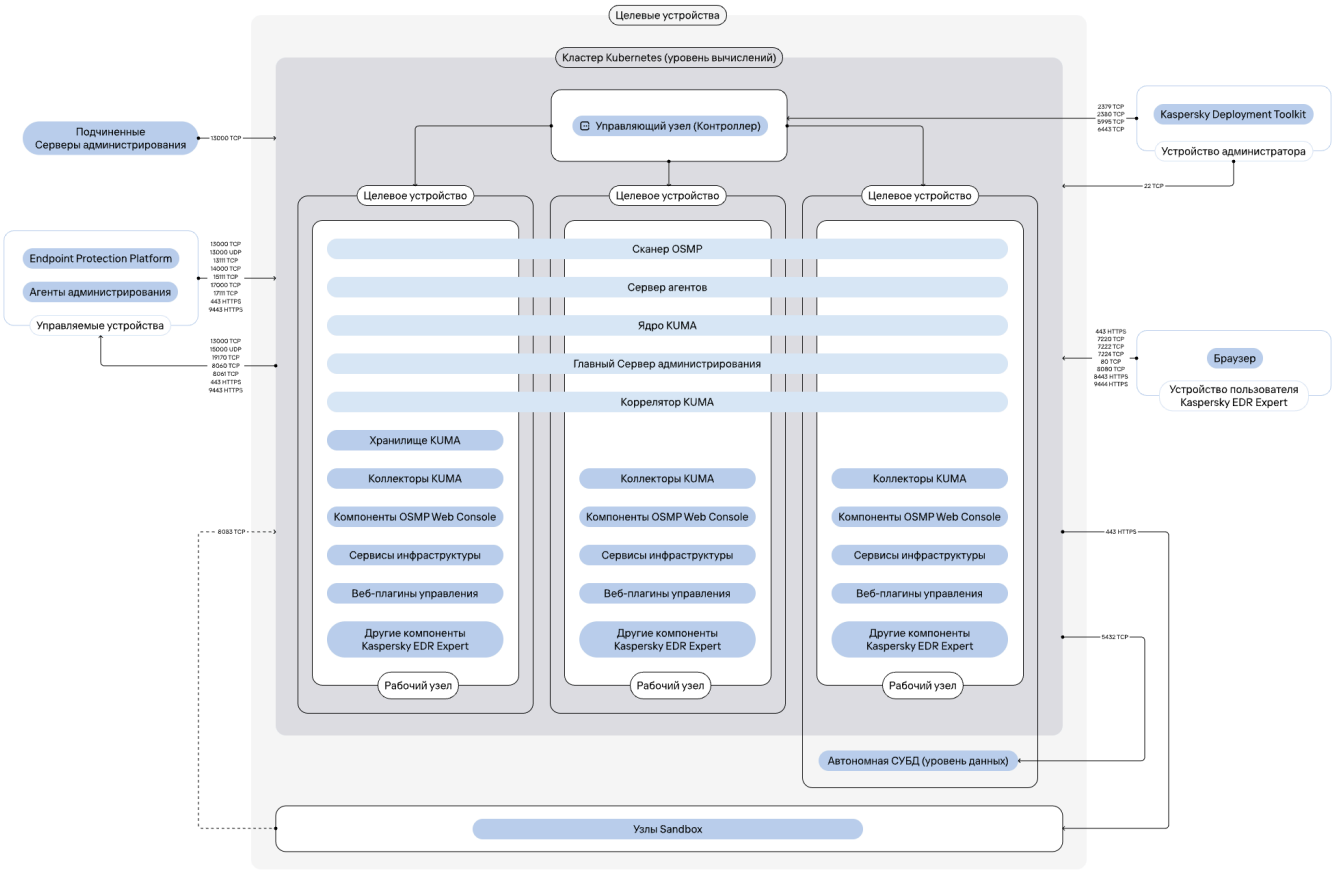


Схема развертывания Kaspersky EDR Expert на нескольких узлах

Схема развертывания Kaspersky EDR Expert на нескольких узлах включает следующие основные элементы:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Этот хост может быть частью кластера Kubernetes, созданного KDT во время развертывания, или может оставаться отдельным.

- **Сервер агентов**. Этот компонент отвечает за взаимодействие между OSMP и приложениями Endpoint Agent.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Кластер Kubernetes**. Кластер Kubernetes включает узел контроллера (также называемый управляющим узлом во время развертывания) и как минимум три рабочих узла. Количество управляющих и рабочих узлов может различаться в зависимости от требований развертывания. На диаграмме показан пример распределения компонентов Kaspersky EDR Expert по рабочим узлам (фактическое распределение может отличаться).

  Автономная СУБД. Система управления базами данных (СУБД) необходима для корректной работы компонентов Kaspersky EDR Expert. Администратор устанавливает СУБД на том же физическом хосте, что и рабочий узел Kubernetes. СУБД нельзя развертывать в кластере Kubernetes – он работает независимо от Orchestration.

- **Ядро KUMA**. Центральный компонент SIEM (KUMA), на основе которого строятся все остальные службы и компоненты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Коллектор KUMA**. Компонент SIEM (KUMA), который получает сообщения из источников событий, обрабатывает их и передает в хранилище KUMA и коррелятор KUMA.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться, как и количество реплик.

- **Коррелятор KUMA**. Компонент SIEM (KUMA), анализирующий нормализованные события.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

- **Хранилище KUMA**. Компонент SIEM (KUMA), используемый для хранения нормализованных событий, что обеспечивает непрерывный и эффективный доступ к ним для аналитической обработки.

- **OSMP Scanner**. Компонент, который выполняет проверку файлов с помощью Anti-Malware Engine, YARA и Sandbox, отправляет их на анализ и формирует отчеты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Узлы Sandbox**. Узел Sandbox, который может включать в себя один или несколько серверов, на которых работают компоненты Sandbox, и предоставляет выделенные вычислительные ресурсы, на которых размещаются изолированная среда выполнения и поддерживающие службы. Эти узлы анализирует файлы, ссылки, URL-адреса и другие объекты, попадающие в защищаемую систему. Узлы Sandbox работает независимо от кластера Kubernetes.

  Количество серверов Sandbox может варьироваться в зависимости от загрузки.

- **Веб-плагин управления**. Компонент, который используется для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP.

  Эти компоненты развернуты на всех узлах кластера.

- **Устройство пользователя с Kaspersky EDR Expert**. Пользовательское устройство, которое используется для входа в Консоль OSMP.

- **Подчиненные Серверы администрирования** (необязательно). Эти серверы используются для создания иерархии Серверов.

- **Управляемые устройства**. Клиентские устройства защищены Kaspersky EDR Expert. На каждом управляемом устройстве установлен Агент администрирования и EPP-приложение.

- **Инфраструктурные сервисы и другие компоненты Kaspersky EDR Expert**. Решение также включает в себя дополнительные компоненты, обеспечивающие централизованное управление активами, обмен данными, построение иерархии, аутентификацию и авторизацию. Другие функции включают в себя аудит действий, управление политиками безопасности и распространение обновлений.

Порты

Схема развертывания не включает все порты, необходимые для успешной установки и работы. Полный список портов приведен в разделе Порты, используемые Kaspersky EDR Expert.

Развертывание на нескольких узлах: схема профиля на шести узлах

Профиль развертывания на шести узлах предназначен для сред с высокими вычислительными потребностями и строгими требованиями к производительности обработки данных. Архитектура с шестью узлами оптимизирована для достижения максимальной производительности за счет разделения сервисов и изоляции интенсивных операций дискового ввода-вывода.

Ключевой особенностью этого профиля является вынесение сервисов SIEM (KUMA) за пределы кластера Kubernetes на выделенные физические или виртуальные серверы. Такой подход устраняет конкуренцию за ресурсы между компонентами и гарантирует стабильную и предсказуемую работу системы при высокой нагрузке.

На рисунке ниже показана схема развертывания Kaspersky EDR Expert на шести узлах.

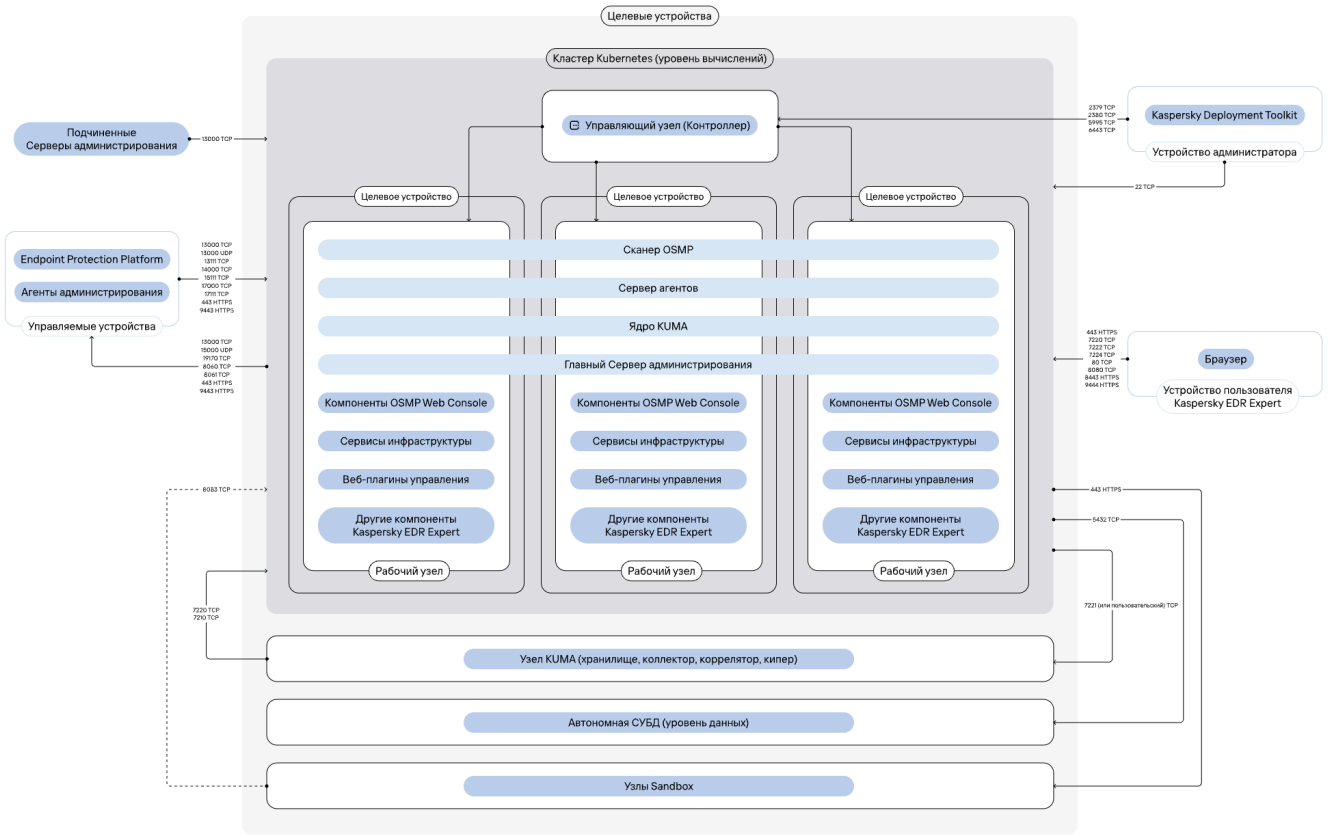


Схема развертывания Kaspersky EDR Expert на нескольких узлах

Схема развертывания Kaspersky EDR Expert на нескольких узлах включает следующие основные элементы:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Этот хост может быть частью кластера Kubernetes, созданного KDT во время развертывания, или может оставаться отдельным.

- **Сервер агентов**. Этот компонент отвечает за взаимодействие между OSMP и приложениями Endpoint Agent.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Кластер Kubernetes**. Кластер Kubernetes включает узел контроллера (также называемый управляющим узлом во время развертывания) и как минимум три рабочих узла. Количество управляющих и рабочих узлов может различаться в зависимости от требований развертывания. На диаграмме показан пример распределения компонентов Kaspersky EDR Expert по рабочим узлам (фактическое распределение может отличаться).

  Автономная СУБД. Система управления базами данных (СУБД) необходима для корректной работы компонентов Kaspersky EDR Expert. Администратор устанавливает СУБД на том же физическом хосте, что и рабочий узел Kubernetes. СУБД нельзя развертывать в кластере Kubernetes – он работает независимо от Orchestration.

- **Ядро KUMA**. Центральный компонент SIEM (KUMA), на основе которого строятся все остальные службы и компоненты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Коллектор KUMA**. Компонент SIEM (KUMA), который получает сообщения из источников событий, обрабатывает их и передает в хранилище KUMA и коррелятор KUMA.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться, как и количество реплик.

- **Коррелятор KUMA**. Компонент SIEM (KUMA), анализирующий нормализованные события.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

- **Хранилище KUMA**. Компонент SIEM (KUMA), используемый для хранения нормализованных событий, что обеспечивает непрерывный и эффективный доступ к ним для аналитической обработки.

- **OSMP Scanner**. Компонент, который выполняет проверку файлов с помощью Anti-Malware Engine, YARA и Sandbox, отправляет их на анализ и формирует отчеты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Узлы Sandbox**. Узел Sandbox, который может включать в себя один или несколько серверов, на которых работают компоненты Sandbox, и предоставляет выделенные вычислительные ресурсы, на которых размещаются изолированная среда выполнения и поддерживающие службы. Эти узлы анализирует файлы, ссылки, URL-адреса и другие объекты, попадающие в защищаемую систему. Узлы Sandbox работает независимо от кластера Kubernetes.

  Количество серверов Sandbox может варьироваться в зависимости от загрузки.

- **Веб-плагин управления**. Компонент, который используется для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP.

  Эти компоненты развернуты на всех узлах кластера.

- **Устройство пользователя с Kaspersky EDR Expert**. Пользовательское устройство, которое используется для входа в Консоль OSMP.

- **Подчиненные Серверы администрирования** (необязательно). Эти серверы используются для создания иерархии Серверов.

- **Управляемые устройства**. Клиентские устройства защищены Kaspersky EDR Expert. На каждом управляемом устройстве установлен Агент администрирования и EPP-приложение.

- **Инфраструктурные сервисы и другие компоненты Kaspersky EDR Expert**. Решение также включает в себя дополнительные компоненты, обеспечивающие централизованное управление активами, обмен данными, построение иерархии, аутентификацию и авторизацию. Другие функции включают в себя аудит действий, управление политиками безопасности и распространение обновлений.

Порты

Схема развертывания не включает все порты, необходимые для успешной установки и работы. Полный список портов приведен в разделе Порты, используемые Kaspersky EDR Expert.

Развертывание с высокой доступностью: схема профиля на 14 узлах

Схема развертывания с высокой доступностью предназначена для систем, требующих непрерывной работы и отказоустойчивости. Эта архитектура основана на принципе дублирования всех критически важных компонентов, благодаря чему в случае отказа сервера его функции автоматически передаются резервному узлу.

На рисунке ниже показана схема развертывания Kaspersky EDR Expert на 14 узлах.

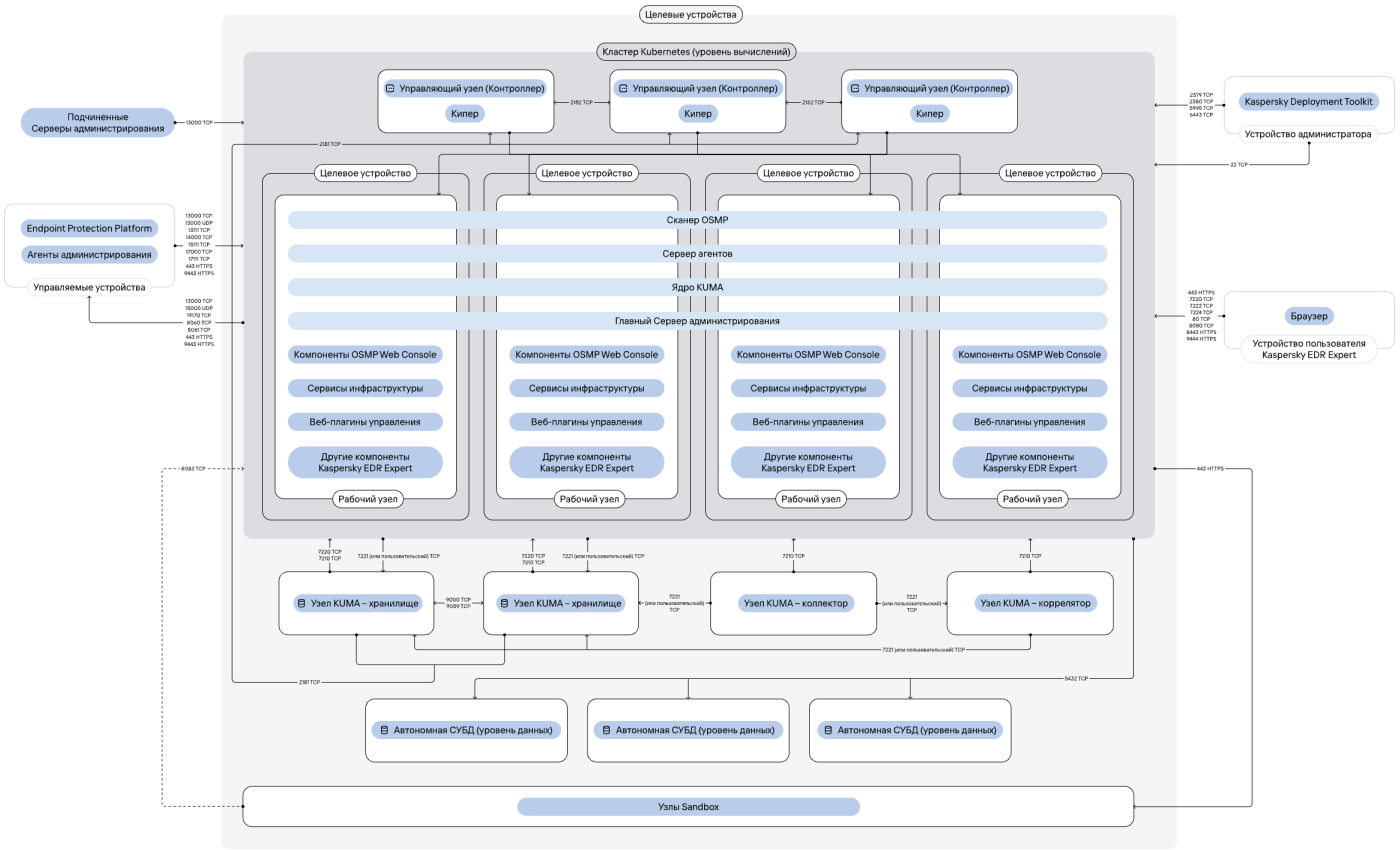


Схема развертывания Kaspersky EDR Expert с высокой доступностью

Схема развертывания Kaspersky EDR Expert с высокой доступностью включает следующие основные компоненты:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Этот хост может быть частью кластера Kubernetes, созданного KDT во время развертывания, или может оставаться отдельным.

- **Сервер агентов**. Этот компонент отвечает за взаимодействие между OSMP и приложениями Endpoint Agent.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Кластер Kubernetes**. Кластер Kubernetes включает узел контроллера (также называемый управляющим узлом во время развертывания) и как минимум три рабочих узла. Количество управляющих и рабочих узлов может различаться в зависимости от требований развертывания. На диаграмме показан пример распределения компонентов Kaspersky EDR Expert по рабочим узлам (фактическое распределение может отличаться).

  Автономная СУБД. Система управления базами данных (СУБД) необходима для корректной работы компонентов Kaspersky EDR Expert. Администратор устанавливает СУБД на том же физическом хосте, что и рабочий узел Kubernetes. СУБД нельзя развертывать в кластере Kubernetes – он работает независимо от Orchestration.

- **Ядро KUMA**. Центральный компонент SIEM (KUMA), на основе которого строятся все остальные службы и компоненты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Коллектор KUMA**. Компонент SIEM (KUMA), который получает сообщения из источников событий, обрабатывает их и передает в хранилище KUMA и коррелятор KUMA.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться, как и количество реплик.

- **Коррелятор KUMA**. Компонент SIEM (KUMA), анализирующий нормализованные события.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

- **Хранилище KUMA**. Компонент SIEM (KUMA), используемый для хранения нормализованных событий, что обеспечивает непрерывный и эффективный доступ к ним для аналитической обработки.

- **OSMP Scanner**. Компонент, который выполняет проверку файлов с помощью Anti-Malware Engine, YARA и Sandbox, отправляет их на анализ и формирует отчеты.

  Распределение компонентов, показанное на диаграмме выше, предназначено исключительно для ознакомления. Фактическое распределение по рабочим узлам может отличаться.

  Этот компонент разворачивается на одном рабочем узле без привязки к узлам. Планировщик Kubernetes выбирает рабочий узел на основе доступных ресурсов.

- **Узлы Sandbox**. Узел Sandbox, который может включать в себя один или несколько серверов, на которых работают компоненты Sandbox, и предоставляет выделенные вычислительные ресурсы, на которых размещаются изолированная среда выполнения и поддерживающие службы. Эти узлы анализирует файлы, ссылки, URL-адреса и другие объекты, попадающие в защищаемую систему. Узлы Sandbox работает независимо от кластера Kubernetes.

  Количество серверов Sandbox может варьироваться в зависимости от загрузки.

- **Веб-плагин управления**. Компонент, который используется для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP.

  Эти компоненты развернуты на всех узлах кластера.

- **Устройство пользователя с Kaspersky EDR Expert**. Пользовательское устройство, которое используется для входа в Консоль OSMP.

- **Подчиненные Серверы администрирования** (необязательно). Эти серверы используются для создания иерархии Серверов.

- **Управляемые устройства**. Клиентские устройства защищены Kaspersky EDR Expert. На каждом управляемом устройстве установлен Агент администрирования и EPP-приложение.

- **Инфраструктурные сервисы и другие компоненты Kaspersky EDR Expert**. Решение также включает в себя дополнительные компоненты, обеспечивающие централизованное управление активами, обмен данными, построение иерархии, аутентификацию и авторизацию. Другие функции включают в себя аудит действий, управление политиками безопасности и распространение обновлений.

Порты

Схема развертывания не включает все порты, необходимые для успешной установки и работы. Полный список портов приведен в разделе Порты, используемые Kaspersky EDR Expert.

Развертывание в нескольких ЦОД

На схеме ниже представлена концептуальная архитектура распределенного развертывания платформы в нескольких ЦОД, при которой сервисы KUMA вынесены за пределы кластера Kubernetes.

Службы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на рабочих узлах, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его. На схеме сервисы KUMA вынесены за пределы кластера Kubernetes.

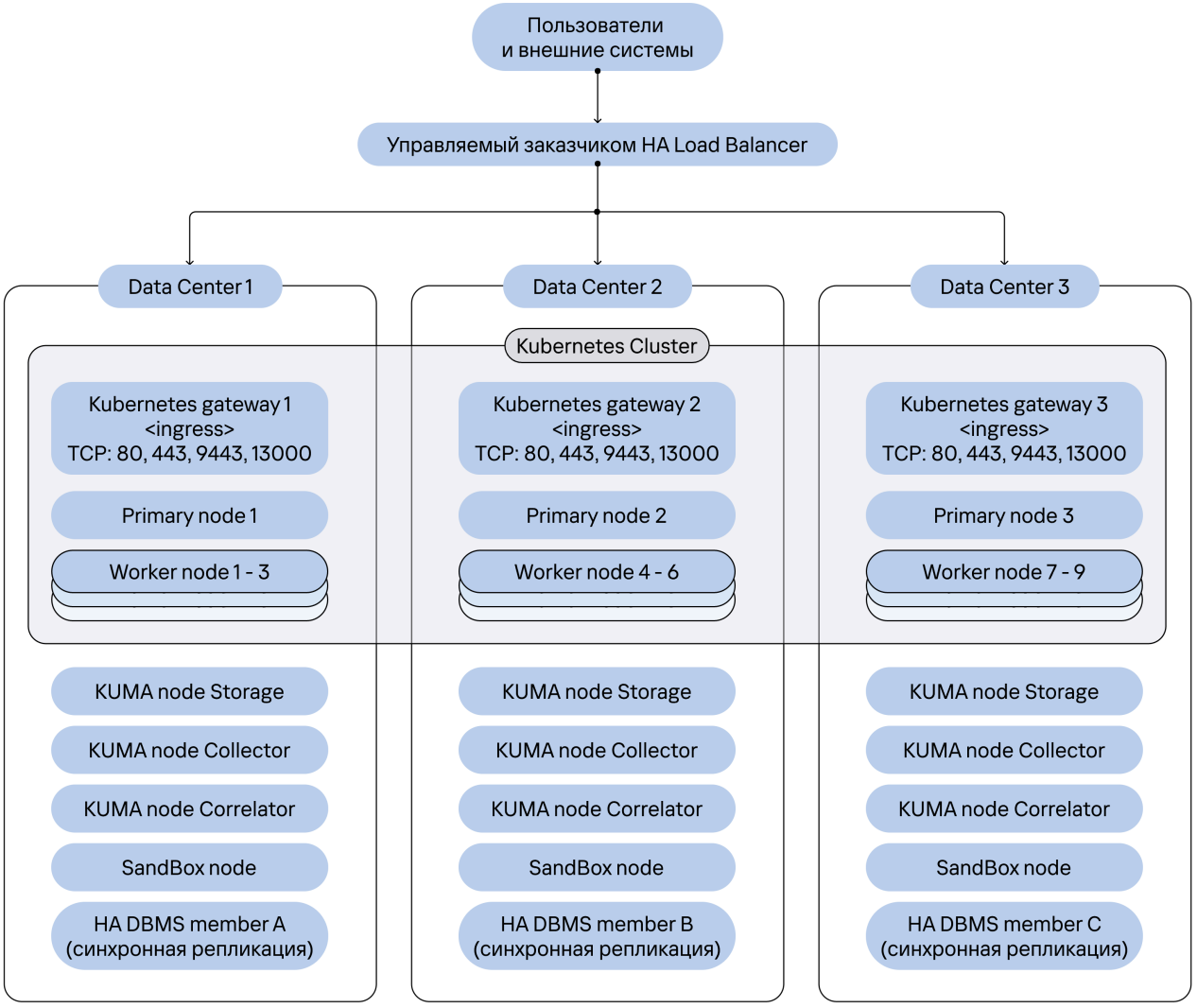


Схема развертывания Kaspersky EDR Expert в нескольких ЦОД

Схема развертывания Kaspersky EDR Expert в нескольких ЦОД включает следующие основные элементы:

- **Кластер Kubernetes**. Кластер Kubernetes включает 3 управляющих узла (не менее 1 узла на каждый центр обработки данных) и 9 рабочих узлов (не менее 3 узлов на каждый центр обработки данных).

- **СУБД**. Система управления базами данных (СУБД) необходима для корректной работы компонентов Kaspersky EDR Expert. СУБД разворачивается в одной из поддерживаемых отказоустойчивых конфигураций. СУБД нельзя развертывать в кластере Kubernetes.

- **Коллектор KUMA**. Компонент SIEM (KUMA), который получает сообщения из источников событий, обрабатывает их и передает в хранилище KUMA и коррелятор KUMA.

- **Коррелятор KUMA**. Компонент SIEM (KUMA), анализирующий нормализованные события.

- **Хранилище KUMA**. Компонент SIEM (KUMA), используемый для хранения нормализованных событий, что обеспечивает непрерывный и эффективный доступ к ним для аналитической обработки.

- **Узлы Sandbox**. Узел Sandbox, который может включать в себя один или несколько серверов, на которых работают компоненты Sandbox, и предоставляет выделенные вычислительные ресурсы, на которых размещаются изолированная среда выполнения и поддерживающие службы. Эти узлы анализирует файлы, ссылки, URL-адреса и другие объекты, попадающие в защищаемую систему. Узлы Sandbox работает независимо от кластера Kubernetes.

  При развертывании в нескольких ЦОД требуется три устройства Sandbox (не менее одного узла на каждый центр обработки данных).

- **Управляемые устройства**. Клиентские устройства защищены Kaspersky EDR Expert. На каждом управляемом устройстве установлен Агент администрирования и EPP-приложение.

- **Инфраструктурные сервисы и другие компоненты Kaspersky EDR Expert**. Решение также включает в себя дополнительные компоненты, обеспечивающие централизованное управление активами, обмен данными, построение иерархии, аутентификацию и авторизацию. Другие функции включают в себя аудит действий, управление политиками безопасности и распространение обновлений.

- **Отказоустойчивый балансировщик нагрузки**. Предназначен для распределения входящего трафика между узлами кластера, расположенными в нескольких центрах обработки данных.

Порты

Схема развертывания не включает все порты, необходимые для успешной установки и работы. Полный список портов приведен в разделе Порты, используемые Kaspersky EDR Expert.

Порты, используемые Kaspersky EDR Expert

Для правильного взаимодействия между устройством администратора и целевыми устройствами вам нужно предоставить доступ к соединению между устройством администратора и целевыми устройствами через порты, перечисленные в таблице ниже. Эти порты невозможно изменить.

Для взаимодействия между устройством администратора и устройствами, которые используются для установки сервисов KUMA и находятся вне кластера Kubernetes, доступ предоставляется только по TCP-порту 22.

Порты, используемые для взаимодействия между устройством администратора и целевыми устройствами

Порт	Протокол	Направление	Source	Назначение	Назначение порта
22	TCP	Входящий	Устройство администратора	Целевые устройства	Обеспечение SSH-соединения от устройства администратора к целевым устройствам. Обеспечение SSH-соединения от устройства администратора к устройствам, которые используются для установки внешних сервисов KUMA.
2379, 2380	TCP	Входящий	Устройство администратора	Целевое устройство (управляющий узел)	Подключение к хранилищу Kubernetes (ETCD).
5995	TCP	Входящий	Устройство администратора	Целевое устройство (управляющий узел)	Подключение к реестру Docker.
6443	TCP	Входящий	Устройство администратора	Целевое устройство (управляющий узел)	Подключение к Kubernetes API.

Для корректной работы компонентов Kaspersky EDR Expert целевые устройства должны находиться в одном широковещательном домене.

В таблице ниже указаны порты, которые должны быть открыты на сетевых экранах всех целевых устройств кластера. Эти порты невозможно изменить.

Если вы используете сетевой экран firewalld или UFW на целевых устройствах, KDT автоматически откроет требуемые порты на сетевых экранах. Или вы можете вручную открыть перечисленные порты перед развертыванием Kaspersky EDR Expert.

Обязательные порты, используемые компонентами Kaspersky EDR Expert

Порт	Протокол	Направление	Source	Назначение	Назначение порта
80, 8080	TCP (HTTP)	Входящий	Браузер	Целевое устройство кластера	Прием соединений от браузера. Перенаправление на порт 443 TCP (HTTPS).
443, 8443	TCP (HTTPS)	Входящий	Браузер	Целевое устройство кластера	Прием соединений от браузера. Прием соединений от Сервера администрирования по OpenAPI. Используется для автоматизации сценариев работы с Сервером администрирования.
13000	TCP	Входящий	Агент администрирования или Сервер администрирования	Целевое устройство кластера	Прием соединений от Агентов администрирования и подчиненных Серверов администрирования.
13000	UDP	Входящий	Агент администрирования;	Целевое устройство кластера	Прием информации от Агентов администрирования о выключении устройств.
14000	TCP	Входящий	Агент администрирования;	Целевое устройство кластера	Прием подключений от Агентов администрирования.
17000	TCP	Входящий	Управляемые устройства	Целевое устройство кластера	Прием подключений для активации приложений от управляемых устройств (кроме мобильных устройств).
19170	TCP (HTTPS)	Исходящий	Целевое устройство кластера	Управляемые устройства	Удаленный доступ к управляемым устройствам с помощью Консоли OSMP.
7210	TCP	Входящий	Целевые устройства KUMA	Целевое устройство кластера	Получение конфигурации KUMA с сервера Ядра KUMA.
7220	TCP	Входящий	Браузер	Целевое устройство кластера	Прием соединений от браузера.
7222	TCP	Входящий	Браузер	Целевое устройство кластера	Реверсивный прокси в системе CyberTrace.
7224	TCP	Входящий	Браузер	Целевое устройство кластера	Ответные вызовы для Identity and Access Manager (IAM).

В таблице ниже указаны порты, которые по умолчанию не открываются на сетевых экранах при развертывании Kaspersky EDR Expert. Эти порты невозможно изменить.

Если вам нужно выполнить действия, перечисленные в столбце **Назначение порта** в таблице ниже, вы можете открыть соответствующие порты на сетевых экранах всех целевых устройств вручную.

Необязательные порты на сетевом экране, используемые компонентами Kaspersky EDR Expert

Порт	Протокол	Направление	Source	Назначение	Назначение порта
8060	TCP	Исходящий	Целевое устройство кластера	Управляемые устройства	Передача опубликованных инсталляционных пакетов на управляемые устройства.
8061	TCP	Исходящий	Целевое устройство кластера	Управляемые устройства	Передача опубликованных инсталляционных пакетов на управляемые устройства.

Порт	Протокол	Направление	Source	Назначение	Назначение порта
8083	HTTP	Входящий	Sandbox	Целевое устройство кластера	Обновление антивирусных баз в Sandbox.
13111	TCP	Входящий	Управляемые устройства	Целевое устройство кластера	Прием запросов от управляемых устройств к прокси-серверу KSN.
15111	UDP	Входящий	Управляемые устройства	Целевое устройство кластера	Прием запросов от управляемых устройств к прокси-серверу KSN.
17111	TCP	Входящий	Управляемые устройства	Целевое устройство кластера	Прием запросов от управляемых устройств к прокси-серверу KSN.
5432	TCP	Входящий	СУБД (PostgreSQL)	Целевое устройство кластера	Взаимодействие с СУБД (PostgreSQL). Этот порт используется, только если вы выполняете демонстрационное развертывание и устанавливаете СУБД на целевом устройстве внутри кластера Kubernetes.

В таблице ниже указаны порты, которые должны быть открыты на сетевых экранах устройств, взаимодействующих с Sandbox.

Порты, используемые для взаимодействия с Sandbox

Порт	Протокол	Направление	Source	Назначение	Назначение порта
22	TCP	Входящий	Устройство администратора	Узел Sandbox	Подключение к серверу Sandbox по протоколу SSH.
443	TCP	Входящий	OSMP	Целевой компонент на узле Sandbox	Входящие соединения от компонентов OSMP.
8443	TCP	Входящий	Браузер	Целевой компонент на узле Sandbox	Доступ к веб-интерфейсу Sandbox.
80 или 443	TCP	Исходящий	Целевой компонент на узле Sandbox	Целевой сервер обновлений	Получение обновлений с серверов обновлений "Лаборатории Касперского".
Любой	Любой	Исходящий и соответствующий входящий	Целевой компонент на узле Sandbox	Целевой ресурс в интернете	Доступ в сеть интернет для анализа сетевого поведения исследуемых объектов.

В таблице ниже указаны порты, которые необходимо открыть для работы кластера Kubernetes и компонентов инфраструктуры. Эти порты невозможно изменить.

Если вы используете сетевой экран firewalld или UFW на целевых устройствах, KDT автоматически откроет требуемые порты на сетевых экранах. Или вы можете вручную открыть перечисленные порты перед развертыванием Kaspersky EDR Expert.

Порты, используемые кластером Kubernetes и компонентами инфраструктуры

Порт	Протокол	Узел
80	TCP	Управляющий узел
443	TCP	Управляющий узел
10250	TCP	Управляющий узел
9443	TCP	Управляющий узел
6443	TCP	Управляющий узел
8132	TCP	Управляющий узел
5995	TCP	Управляющий узел
80	TCP	Рабочий узел
443	TCP	Рабочий узел

Порт	Протокол	Узел
179	TCP	Рабочий узел
10250	TCP	Рабочий узел
10255	TCP	Рабочий узел
9443	TCP	Рабочий узел
6443	TCP	Рабочий узел
9500	TCP	Рабочий узел
9501	TCP	Рабочий узел
9502	TCP	Рабочий узел
9503	TCP	Рабочий узел
8500	TCP	Рабочий узел
8501	TCP	Рабочий узел
3260	TCP	Рабочий узел
8000	TCP	Рабочий узел
8002	TCP	Рабочий узел
2049	TCP	Рабочий узел
3370	TCP	Рабочий узел
179	UDP	Рабочий узел
51820	UDP	Рабочий узел
51821	UDP	Рабочий узел

Для корректной работы сервисов KUMA, не входящих в кластер Kubernetes, вам нужно открыть порты, указанные в таблице ниже. В таблице ниже показаны значения сетевых портов по умолчанию. Эти порты автоматически открываются во время установки KUMA.

Порты, используемые для взаимодействия с внешними сервисами KUMA

Порт	Протокол	Направление	Source	Назначение	Назначение порта
8123	HTTPS	Входящий	Сервис хранилища	Узел кластера ClickHouse	Запись и получение нормализованных событий в кластере ClickHouse.
9009	HTTPS	Входящий/ Исходящий	Реплика кластера ClickHouse	Реплика кластера ClickHouse	Внутренняя связь между репликами кластера ClickHouse для передачи данных кластера.
2181	TCP	Входящий	Узлы кластера ClickHouse	Служба координации для репликации данных ClickHouse	Получение и запись метаданных репликации репликами серверов ClickHouse.
2182	TCP	Входящий/ Исходящий	Служба координации для репликации данных ClickHouse	Служба координации для репликации данных ClickHouse	Внутренняя связь между службами координации репликации для достижения кворума.
8001	TCP	Входящий	VictoriaMetrics	Сервер ClickHouse	Получение метрик работы сервера ClickHouse.
9000	TCP	Входящий	Клиент ClickHouse	Узел кластера ClickHouse	Запись и получение данных в кластере ClickHouse.

Если вы создаете дополнительный сервис KUMA (коллектор, коррелятор или хранилище) на сервере, вам необходимо вручную открыть порт, соответствующий созданному сервису на сервере. Вы можете использовать порт TCP 7221 или другой порт, используемый для установки службы.

Если используются стандартные примеры служб, при развертывании Kaspersky EDR Expert автоматически открываются следующие порты:

- 7230 TCP
- 7231 TCP
- 7232 TCP
- 7233 TCP
- 7234 TCP
- 7235 TCP
- 7236 TCP
- 5140 TCP
- 5140 UDP
- 5141 TCP
- 5144 UDP
- 5150 UDP

Изменение порта, используемого для подключения к серверу Консоли OSMP

Тот же узел и порт (443) используются по умолчанию, когда администратор подключается к серверу Консоли OSMP с помощью браузера и когда Endpoint Agents подключаются к компоненту agentserver, хотя для каждого подключения используются разные FQDN. При необходимости два разных порта для этих компонентов можно настроить во время установки Kaspersky EDR Expert или уже после установки решения.

Чтобы изменить требуемый порт, необходим доступ к устройству администратора, на котором размещена утилита KDT.

Процедуры изменения порта Консоли OSMP имеют следующие ограничения:

- Если в качестве номера порта вы укажете недопустимое значение (вне диапазона, с недопустимыми символами или пустое), установка решения завершится ошибкой.
- После изменения порта всегда указывайте новый номер порта в адресной строке браузера при подключении к Консоли OSMP.

Чтобы изменить порт Консоли OSMP, когда Kaspersky EDR Expert уже установлен, выполните следующие действия:

1. Выберите новый номер порта в диапазоне 1–65535.

2. Если вы используете сетевой экран или другие инструменты, ограничивающие доступ к сети, настройте их таким образом, чтобы выбранный порт был доступен.

3. Выполните следующую команду, чтобы изменить порт:

   ```
   ./kdt invoke foreach -a setConsolePort --param console_port="<port_number>"
   ```

   где `<port_number>` нужно будет заменить выбранным номером порта.

   Если команда выполнена успешно, текущие сеансы подключения к Консоли OSMP будут завершены.

4. Повторно подключитесь к серверу Консоли OSMP. Для этого в адресной строке браузера введите FQDN службы Web Console, указанный в конфигурационном файле, и новый номер порта.

Порт для подключения к Консоли OSMP будет изменен. Порт по умолчанию (443) больше не будет принимать подключения к Консоли OSMP.

Чтобы изменить порт Консоли OSMP во время установки Kaspersky EDR Expert:

1. Выберите новый номер порта в диапазоне 1–65535.

2. Укажите новый номер порта в конфигурационном файле.

   Для этого добавьте параметр установки для нового порта Консоли OSMP в конфигурационный файл, а затем укажите номер выбранного порта следующим образом:

   ```
   parameters:
     - name: console_port
       source:
         value: "<port_number>"
   ```

   где:

   - `console_port` – новый номер порта.
   - `<port_number>` нужно будет заменить выбранным номером порта.

3. Если вы используете сетевой экран или другие инструменты, ограничивающие доступ к сети, настройте их таким образом, чтобы выбранный порт был доступен.

4. Установите Kaspersky EDR Expert.

   Дополнительную информацию см. в разделе Развертывание Kaspersky EDR Expert.

5. После завершения установки подключитесь к серверу Консоли OSMP.

   Для этого в адресной строке браузера введите FQDN службы Web Console и новый номер порта, указанный в конфигурационном файле.

Порт для подключения к Консоли OSMP будет изменен. Порт по умолчанию (443) больше не будет использоваться для подключения к Консоли OSMP.

Изменение порта, используемого Endpoint Agents для подключения к компоненту agentserver

Тот же узел и порт (443) используются по умолчанию, когда администратор подключается к серверу Консоли OSMP с помощью браузера и когда Endpoint Agents подключаются к компоненту agentserver, хотя для каждого подключения используются разные FQDN. При необходимости два разных порта для этих компонентов можно настроить во время установки Kaspersky EDR Expert или уже после установки решения.

Чтобы изменить требуемый порт, необходим доступ к устройству администратора, на котором размещена утилита KDT, а также права на изменение политики Endpoint Agents.

Процедуры изменения порта, используемого Endpoint Agents, имеет ограничение.Если в качестве номера порта вы укажете недопустимое значение (вне диапазона, с недопустимыми символами или пустое), команда на изменение порта будет выполнена с ошибкой в ходе первой процедуры. Во второй процедуре установка решения завершится ошибкой.

Чтобы изменить порт, используемый Endpoint Agents, когда Kaspersky EDR Expert уже установлен, выполните следующие действия:

1. Выберите новый номер порта в диапазоне 1–65535.

2. Если вы используете сетевой экран или другие инструменты, ограничивающие доступ к сети, настройте их таким образом, чтобы выбранный порт был доступен.

3. Выполните следующие команды, чтобы изменить порт, используемый Endpoint Agents для подключения к компоненту agentserver (первая команда), и порт, используемый для отправки телеметрии (вторая команда):

   ```
   ./kdt invoke foreach -a changeAgentServerSmpPort --param as_smp_port="<port_number>"
   ```

   ```
   ./kdt invoke foreach -a setKumaTelemetryPort --param kuma_gateway_telemetry_listener_port="<port_number>"
   ```

   где `<port_number>` нужно будет заменить выбранным номером порта.

   Если команды выполнены успешно, текущие сеансы подключения между Endpoint Agents и компонентом agentserver будут завершены. Компонент agentserver больше не будет получает данные от Endpoint Agents.

4. Если данные от Endpoint Agents маршрутизируются через прокси-узел, выполните следующие действия:

   a. В конфигурационном файле Nginx укажите новый номер порта в строке `listen <port_number> ssl http2;`

   b. Чтобы применить изменения, внесенные в конфигурационный файл, перезапустите Nginx, выполнив команду `nginx -s reload`.

5. В главном меню Консоли OSMP перейдите в **Управление активами** → **Политики**.

6. Нажмите на политику в приложение безопасности интересующей вас Endpoint Agent из списка и перейдите в раздел **Настройка приложения** → **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)** → **Подключение к серверам реагирования**.

7. В разделе **Настройки подключения** установите флажок рядом с сервером и нажмите на кнопку **Удалить**.

   Требуемый сервер со старым портом будет удален.

8. Нажмите на кнопку **Добавить** на панели, а затем нажмите на кнопку **Выбрать сервер**.

9. В открывшемся окне выберите сервер с новым портом и подтвердите действие.

Порт, используемый Endpoint Agents для подключения к компоненту agentserver, будет изменен. Компонент agentserver начнет получать данные от Endpoint Agents через новый порт. После применения политики к Endpoint Agents они будут повторно подключены к компонентам OSMP через новый порт. Порт по умолчанию (443) больше не будет использоваться для подключения к компоненту agentserver.

Чтобы изменить порт, используемый Endpoint Agents, во время установки Kaspersky EDR Expert:

1. Выберите новый номер порта в диапазоне 1–65535.

2. В файле конфигурации укажите новый порт, используемый Endpoint Agents для подключения компоненту agentserver и порту, используемому для отправки телеметрии.

   Для этого добавьте параметры установки для новых портов в конфигурационный файл следующим образом:

   ```
   parameters:
   - name: as_smp_port
     source:
       value: "<port_number>"
   - name: kuma_gateway_telemetry_listener_port
     source:
       value: "<port_number>"
   ```

   где:

   - `as_smp_port` – новый номер порта, используемый Endpoint Agents.
   - `kuma_gateway_telemetry_listener_port` – новый номер порта, используемый для отправки телеметрии.
   - `<port_number>` нужно будет заменить выбранным номером порта.

3. Если вы используете сетевой экран или другие инструменты, ограничивающие доступ к сети, настройте их таким образом, чтобы выбранный порт был доступен.

4. Установите Kaspersky EDR Expert.

   Дополнительную информацию см. в разделе Развертывание Kaspersky EDR Expert.

5. Если данные от Endpoint Agents маршрутизируются через прокси-узел, выполните следующие действия:

   a. В конфигурационном файле Nginx укажите новый номер порта в строке `listen <port_number> ssl http2;`

   b. Чтобы применить изменения, внесенные в конфигурационный файл, перезапустите Nginx, выполнив команду `nginx -s reload`.

Порт, используемый Endpoint Agents, будет изменен. Компонент agentserver начнет получать данные от Endpoint Agents через новый порт. Порт по умолчанию (443) не будет использоваться для подключения к компоненту agentserver.

Подготовительные работы и развертывание

В этом разделе описано, как подготовить инфраструктуру к развертыванию Kaspersky EDR Expert, настроить параметры установки, необходимые для развертывания на нескольких узлах или развертывания на одном узле, а также как использовать мастер развертывания для создания конфигурационного файла.

Вы узнаете, как установить Kaspersky EDR Expert по схеме развертывания на нескольких узлах и развертывания на одном узле. Также в этом разделе содержится информация о том, как развернуть несколько кластеров Kubernetes с экземплярами Kaspersky EDR Expert и переключаться между ними с помощью KDT.

Развертывание на нескольких узлах: подготовка устройства администратора и целевых устройств

Подготовка к развертыванию на нескольких узлах включает настройку устройства администратора и целевых устройств. После подготовки устройств и указания конфигурационного файла вы сможете развернуть Kaspersky EDR Expert на целевых устройствах с использованием KDT.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert.

Все виртуальные процессоры, назначенные устройству администратора, должны находиться на одном узле NUMA. При настройке виртуальной машины для устройства администратора на гипервизоре убедитесь, что ресурсы процессора и памяти выделяются из одного узла NUMA. Это предотвращает доступ к памяти между узлами, что может вызвать сбои при распределении памяти во время установки.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям.

   Если устройство администратора не входит в кластер Kubernetes, обратитесь к требованиям KDT.

   Если устройство администратора входит в кластер, обратитесь к требованиям к оборудованию для развертывания на нескольких узлах и к программным требованиям OSMP.

2. Выделите не менее 15 ГБ свободного места в директории временных файлов (`/tmp`) для KDT.

   Чтобы выяснить, сколько места доступно в директории `/tmp`, выполните следующую команду:

   ```
   df -h /tmp
   ```

   Если у вас недостаточно свободного места в этой директории, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. Установите пакет для Docker версии 23 или выше. Не устанавливайте неофициальные версии пакета Docker из хранилищ операционных систем.

   На разделе диска для хранения данных Docker (по умолчанию `/var/lib/docker`) должно быть не менее 60 ГБ свободного места.

4. Выполните действия после установки, чтобы настроить устройство администратора для правильной работы с Docker:

   ```
   sudo groupadd docker
   sudo usermod -aG docker $USER
   newgrp docker
   sudo systemctl enable docker.service
   sudo systemctl enable containerd.service
   sudo systemctl status docker.service
   ```

   Убедитесь, что сервис Docker находится в состоянии **Active**.

   Если ключ невозможно скачать автоматически, скачайте его вручную:

   1. Откройте ссылку https://download.docker.com/linux/ubuntu/gpg в браузере и сохраните ключ как docker.asc.

   2. Выполните следующую команду:

      ```
      sudo mv docker.asc /etc/apt/keyrings/docker.asc
      ```

5. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Поскольку устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на нескольких узлах.

   b. Убедитесь, что на устройстве администратора поддерживается технология cgroup v2.

   a. Since the device will act as the administrator and target host, make sure that it meets the requirements for the single-node deployment (because the demonstration and single-node deployment have a similar deployment scheme).

   b. Make sure that the cgroup v2 technology is supported on the administrator host.

      The cgroup v2 technology is supported for the Linux kernel version 2.6.24 or later.

   c. Install the uidmap package on the administrator host.

      Check that the /etc/subgid and /etc/subuid files contain the user account under which KDT will be launched. To do this, you can run the following command:

      ```
      getsubids USER
      ```

      If this command does not return a result, you must add the user account to the /etc/subgid and /etc/subuid files manually in the following format:

      ```
      <username>:<min_subid>:<range_length>
      ```

      where

      - `<username>`—Username of the account under which KDT will be launched.
      - `<min_subid>`—Minimum subuid value.
      - `<range_length>`—Number of subuids allocated for the user `<username>`.

Подготовка целевых устройств

Целевые устройства – это физические или виртуальные машины, которые используются для развертывания Kaspersky EDR Expert и которые включены в кластер Kubernetes. На этих устройствах работают компоненты Kaspersky EDR Expert.

> Одно из целевых устройств может быть использовано в качестве устройства администратора. В этом случае вам необходимо подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, а затем подготовить целевое устройство.

Минимальная конфигурация кластера для развертывания на нескольких узлах включает четыре узла:

- Один управляющий узел.

  Управляющий узел предназначен для управления кластером, хранения метаданных и распределения рабочей нагрузки.

- Три рабочих узла.

  Рабочие узлы предназначены для выполнения рабочей нагрузки компонентов Kaspersky EDR Expert.

Количество первичных и рабочих узлов в кластере может быть разным. Для оптимального распределения нагрузки между узлами рекомендуется использовать узлы с примерно одинаковой производительностью.

Службы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на рабочих узлах, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его.

При наличии нескольких управляющих узлов вам потребуется балансировщик нагрузки для распределения поступающих запросов по управляющим узлам и обеспечения равномерной рабочей нагрузки. Если вы хотите использовать внешний балансировщик нагрузки, выделите отдельное устройство вне кластера Kubernetes и укажите его параметры в файле конфигурации. Если вы не хотите использовать внешний балансировщик нагрузки, его роль будет выполнять рабочий узел.

Чтобы подготовить целевые устройства:

1. Убедитесь, что оборудование и программное обеспечение на целевых устройствах соответствуют требованиям для развертывания на нескольких узлах и целевые устройства расположены в одном широковещательном домене.

   Если сервисы KUMA установлены внутри кластера, целевые устройства должны соответствовать требованиям к оборудованию, программному обеспечению и требованиям к установке, необходимым для установки сервисов KUMA.

   > Для правильной работы Kaspersky EDR Expert версия ядра Linux должна быть 5.15.0.107 или выше на целевых устройствах с операционной системой семейства Ubuntu.

   > Docker не должен быть установлен на целевых устройствах, кроме целевого устройства, которое будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. Убедитесь, что в файловой системе, смонтированной в `/var`, на каждом целевом устройстве есть не менее 700 ГБ свободного дискового пространства.

   Чтобы выяснить, сколько места доступно в директории `/var`, выполните следующую команду:

   ```
   df -h /var
   ```

3. Убедитесь, что на каждом целевом хосте установлен пакет sudo:

   ```
   apt list --installed | grep sudo
   ```

   В выводе команды должны быть перечислены пакеты с указанным именем пакета, например:

   ```
   sudo/noble-updates,noble-security,now 1.9.15p5-3ubuntu5.24.04.2 amd64 [installed]
   ```

   Установите пакет sudo, если этот пакет еще не установлен:

   ```
   apt install sudo
   ```

4. Для операционных систем семейства Debian установите пакет UFW:

   ```
   apt install ufw
   ```

5. На каждом целевом устройстве настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, настройте доступ в интернет, используя прокси-сервер на целевых устройствах.

6. Если на управляющем рабочем узле используется UFW, разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

7. Предоставьте доступ к хранилищу пакетов, в котором хранятся следующие пакеты, необходимые для Kaspersky EDR Expert:

   - nfs-common;
   - cron;
   - tar;
   - open-iscsi;
   - python3-cffi-backend;
   - python3-cryptography;
   - systemd;
   - cryptsetup-bin;
   - cryptsetup;
   - netcat-traditional;
   - containerd.

   KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

8. Убедитесь, что на каждом целевом узле установлены пакеты python3-apt и libnfs:

   ```
   apt list --installed | grep <название_пакета>
   ```

   В выводе команды должны быть перечислены пакеты с указанным именем пакета, например:

   ```
   libnfs14/noble,now 5.0.2-1build1 amd64 [installed,automatic]
   libnfsidmap1/noble-updates,now 1:2.6.4-3ubuntu5.1 amd64 [installed,automatic]
   ```

   Пакеты python3-apt и libnfs не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены. Используется пакет libnfs версии 12 и выше.

   ```
   sudo apt install <название_пакета>
   ```

9. Для управляющих узлов убедитесь, что установлен пакет curl.

   Пакет curl не устанавливается во время развертывания из репозитория пакетов с помощью KDT. Этот пакет необходимо установить вручную, если он еще не установлен.

10. Убедитесь, что конфигурационные файлы не ссылаются на какие-либо недоступные репозитории: команда `apt update` не должна возвращать ошибок.

11. Отключите защиту от ARP-спуфинга на гипервизоре или в сетевой инфраструктуре для целевых хостов.

12. Зарезервируйте статические IP-адреса для целевых устройств и шлюза кластера Kubernetes.

    Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. IP-адрес шлюза является IPv4-адресом (например, 10.80.23.182). IP-адрес шлюза указан в конфигурационном файле (параметр `ingress_ip`).

    Убедитесь, что целевые устройства, шлюз соединения кластера Kubernetes и устройство с СУБД находятся в одном широковещательном домене.

Для шлюза кластера Kubernetes и целевых устройств требуется IPv4-адресация. Если в вашей среде требуется подключение по протоколу IPv6, настройте операционные системы на целевых устройствах и шлюзе кластера Kubernetes для маршрутизации трафика IPv6 через шлюз IPv6 (NAT64) или туннель IPv6. Эта конфигурация поддерживает работу кластера на IPv4, обеспечивая взаимодействие с сетями IPv6.

13. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Kaspersky EDR Expert.

    По умолчанию службы Kaspersky EDR Expert доступны по следующим адресам:

    - <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
    - <ksc_host>.<smp_domain> – взаимодействие с Сервером администрирования.
    - <kuma_host>.<smp_domain> – доступ к компоненту SIEM.
    - <api_host>.<smp_domain> – доступ к API Kaspersky EDR Expert.
    - <monitoring_host>.<smp_domain> – доступ к метрикам OSMP.

      Где <console_host>, <ksc_host>, <kuma_host>, <api_host> и <monitoring_host> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями сервисов FQDN, которые вы можете указать в конфигурационном файле. Если вы не указываете пользовательские значения имен служб устройств, используются значения по умолчанию: `console_host` – "`console`", `ksc_host` – "`admsrv`", `kuma_host` – "`kuma`", `api_host` – "`api`", `monitoring_host` – "`monitoring`".

    Перечисленные FQDN служб должны разрешаться в IP-адрес кластера Kubernetes. Например, если адрес кластера Kubernetes – 10.80.23.182, FQDN служб должны разрешаться в IP-адрес следующим образом:

    - <console_host>.<smp_domain> – 10.80.23.182
    - <ksc_host>.<smp_domain> – 10.80.23.182
    - <kuma_host>.<smp_domain> – 10.80.23.182
    - <api_host>.<smp_domain> – 10.80.23.182
    - <monitoring_host>.<smp_domain> – 10.80.23.182

14. На каждом целевом устройстве создайте учетные записи, которые будут использоваться для развертывания Kaspersky EDR Expert.

    Эти учетные записи используются для SSH-соединения и должны иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

    a. Выполните следующие команды:

    ```
    sudo useradd -m -s /bin/bash sshuser
    sudo usermod -aG sudo sshuser
    ```

    b. Откройте файл /etc/sudoers с помощью команды:

    ```
    sudo visudo
    ```

    c. Добавьте следующую строку в конец файла:

```
sshuser ALL=(ALL) NOPASSWD: ALL
```

Где `sshuser` – имя созданного пользователя.

d. Выполните следующую команду:

```
sudo systemctl restart ssh
```

15. Настройте SSH-соединение между устройством администратора и целевыми устройствами:

a. На устройстве администратора выполните следующую команду, чтобы сгенерировать SSH-ключи с помощью утилиты ssh-keygen без парольной фразы.

```
ssh-keygen -t rsa
```

b. Скопируйте открытый ключ на целевое устройство (например, в директорию `/home/sshuser/.ssh`) с помощью утилиты ssh-copy-id:

```
ssh-copy-id sshuser@<IP_целевого_хоста>
```

Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

Пример создания открытого ключа

Чтобы создать открытый ключ, выполните следующую команду:

```
ssh-keygen -t rsa
ssh-copy-id sshuser@<IP_целевого_хоста>
```

16. Для корректной работы компонентов Kaspersky EDR Expert обеспечьте сетевой доступ между целевыми устройствами и при необходимости откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

17. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

18. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Kaspersky EDR Expert.

Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации, или конечные сертификаты для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Развертывание на одном узле: подготовка устройства администратора и целевых устройств

Подготовка к развертыванию на одном узле включает настройку устройства администратора и целевых устройств. В конфигурации с одним узлом кластер Kubernetes и компоненты Kaspersky EDR Expert устанавливаются на одном целевом устройстве. После подготовки целевого устройства и указания конфигурационного файла, вы сможете развернуть Kaspersky EDR Expert на целевом устройстве с использованием KDT.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert. В этом случае будет использовано только одно устройство для развертывания и работы решения.

> Все виртуальные процессоры, назначенные устройству администратора, должны находиться на одном узле NUMA. При настройке виртуальной машины для устройства администратора на гипервизоре убедитесь, что ресурсы процессора и памяти выделяются из одного узла NUMA. Это предотвращает доступ к памяти между узлами, что может вызвать сбои при распределении памяти во время установки.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям.

   Если устройство администратора не входит в кластер Kubernetes, обратитесь к требованиям KDT.

   Если устройство администратора входит в кластер, обратитесь к требованиям к оборудованию для развертывания на одном узле и к программным требованиям OSMP.

2. Выделите не менее 15 ГБ свободного места в директории временных файлов (`/tmp`) для KDT.

   Чтобы выяснить, сколько места доступно в директории `/tmp`, выполните следующую команду:

   ```
   df -h /tmp
   ```

   Если у вас недостаточно свободного места в этой директории, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<новая_директория>/tmp
   ```

3. Установите Docker.

   Поддерживаются версии Docker 25 и выше.

   На разделе диска для хранения данных Docker (по умолчанию `/var/lib/docker`) должно быть не менее 60 ГБ свободного места.

   Установка Docker на Ubuntu Server 24.04 LTS

   Ниже приведен пример установки Docker на стандартную виртуальную машину Ubuntu Server 24.04 LTS.

   ### Установка на Ubuntu 24.04 LTS

   Выполните следующую команду:

   ```
   sudo apt update && sudo apt install docker.io
   ```

ИЛИ Установка с использованием официальной инструкции

Выполните следующие команды:

1. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

2. Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod
0755 /etc/apt/keyrings/docker.asc
```

3. Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

4. Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-
compose-plugin
```

4. Выполните следующие действия после установки, чтобы настроить устройство администратора для правильной работы с Docker:

```
sudo groupadd docker
sudo usermod -aG docker $USER
newgrp docker
sudo systemctl enable docker.service
sudo systemctl enable containerd.service
sudo systemctl status docker.service
```

Выполните следующую команду, чтобы убедиться, что служба Docker активна:

```
sudo systemctl status docker
```

Если ключ невозможно скачать автоматически, скачайте его вручную:

1. Откройте ссылку https://download.docker.com/linux/ubuntu/gpg в браузере и сохраните ключ как docker.asc.

2. Выполните следующую команду:

```
sudo mv docker.asc /etc/apt/keyrings/docker.asc
```

5. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Так как устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на одном узле.

   b. Убедитесь, что на устройстве администратора технология cgroup v2 поддерживается (присутствует файл `/sys/fs/cgroup/cgroup.controllers`).

Подготовка целевого устройства

Целевое устройство – это физическая или виртуальная машина, которая используются для развертывания Kaspersky EDR Expert и которая включена в кластер Kubernetes. Целевое устройство управляет кластером Kubernetes и компонентами Kaspersky EDR Expert, которые работают на этом устройстве, а также хранит метаданные.

Минимальная конфигурация кластера для развертывания с одним узлом включает одно целевое устройство, которое действует как управляющий и рабочий узлы. На этом управляющем рабочем узле установлен кластер Kubernetes и компоненты Kaspersky EDR Expert.

Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на основном рабочем узле, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его.

> Если вы хотите запустить развертывание Kaspersky EDR Expert с целевого устройства, вам нужно подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, и подготовить целевое устройство.

Чтобы подготовить целевое устройство:

1. Убедитесь, что оборудование и программное обеспечение на целевом устройстве соответствуют требованиям для развертывания на одном узле.

   Если сервисы KUMA будут установлены вне кластера, целевое устройство должно соответствовать требованиям к оборудованию, программному обеспечению и требованиям установки, необходимым для установки сервисов KUMA.

   Поскольку СУБД будет установлена на целевом устройстве, вам также нужно убедиться, что целевое устройство соответствует требованиям для СУБД.

   > Для правильной работы Kaspersky EDR Expert версия ядра Linux должна быть 5.15.0.107 или выше на целевом устройстве с операционной системой семейства Ubuntu.

   > Не устанавливайте Docker на целевом устройстве , если целевое устройство не будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. Убедитесь, что в файловой системе, смонтированной в `/var`, на целевом устройстве есть не менее 360 ГБ свободного дискового пространства.

   Чтобы выяснить, сколько места доступно в директории `/var`, выполните следующую команду:

```
df -h /var
```

3. Настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, настройте доступ в интернет, используя прокси-сервер на целевых устройствах.

4. Убедитесь, что пакет sudo установлен:

   ```
   apt list --installed | grep sudo
   ```

   В выводе команды должны быть перечислены пакеты с указанным именем пакета, например:

   ```
   sudo/noble-updates,noble-security,now 1.9.15p5-3ubuntu5.24.04.2 amd64 [installed]
   ```

   Установите пакет sudo, если этот пакет еще не установлен:

   ```
   apt install sudo
   ```

5. Для операционных систем семейства Debian установите пакет UFW:

   ```
   apt install ufw
   ```

6. Если на управляющем рабочем узле используется UFW, разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

7. Предоставьте доступ к хранилищу пакетов, в котором хранятся следующие пакеты, необходимые для Kaspersky EDR Expert:

   - nfs-common
   - cron
   - tar
   - open-iscsi;
   - python3-cffi-backend
   - python3-cryptography
   - systemd
   - cryptsetup-bin
   - cryptsetup
   - netcat-traditional
   - containerd

   KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

8. Убедитесь, что пакеты python3-apt, curl и libnfs установлены на управляющем рабочем узле:

   ```
   apt list --installed | grep <название_пакета>
   ```

   В выводе команды должны быть перечислены пакеты с указанным именем пакета, например:

   ```
   libnfs14/noble,now 5.0.2-1build1 amd64 [installed,automatic]
   libnfsidmap1/noble-updates,now 1:2.6.4-3ubuntu5.1 amd64 [installed,automatic]
   ```

Пакеты python3-apt, curl и libnfs не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены. Используется пакет libnfs версии 12 и выше.

```
sudo apt install <название_пакета>
```

9. Убедитесь, что конфигурационные файлы не ссылаются на какие-либо недоступные репозитории: команда `apt update` не должна возвращать ошибок.

10. Отключите защиту от ARP-спуфинга на гипервизоре или в сетевой инфраструктуре для целевых устройств.

11. Зарезервируйте статические IP-адреса для целевых устройств и шлюза кластера Kubernetes.

    Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. IP-адрес шлюза является IPv4-адресом (например, 10.80.23.182). IP-адрес шлюза указан в конфигурационном файле (параметр `ingress_ip`). Статический IP-адрес, указанный в параметре `ingress_ip`, должен быть заранее зарезервирован в DNS и оставаться свободным, то есть не должен быть назначен ни одному серверу.

    Убедитесь, что целевое устройство и шлюз соединения кластера Kubernetes находятся в одном широковещательном домене.

    > Для шлюза кластера Kubernetes и целевых устройств требуется IPv4-адресация. Если в вашей среде требуется подключение по протоколу IPv6, настройте операционные системы на целевых устройствах и шлюзе кластера Kubernetes для маршрутизации трафика IPv6 через шлюз IPv6 (NAT64) или туннель IPv6. Эта конфигурация поддерживает работу кластера на IPv4, обеспечивая взаимодействие с сетями IPv6.

12. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Kaspersky EDR Expert.

    По умолчанию службы Kaspersky EDR Expert доступны по следующим адресам:

    - <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
    - <ksc_host>.<smp_domain> – взаимодействие с Сервером администрирования.
    - <kuma_host>.<smp_domain> – доступ к компоненту SIEM.
    - <api_host>.<smp_domain> – доступ к API Kaspersky EDR Expert.
    - <monitoring_host>.<smp_domain> – доступ к метрикам OSMP.

      Где <console_host>, <ksc_host>, <kuma_host>, <api_host> и <monitoring_host> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями сервисов FQDN, которые вы можете указать в конфигурационном файле. Если вы не указываете пользовательские значения имен служб устройств, используются значения по умолчанию: `console_host` – `"console"`, `ksc_host` – `"admsrv"`, `kuma_host` – `"kuma"`, `api_host` – `"api"`, `monitoring_host` – `"monitoring"`.

    Перечисленные FQDN служб должны разрешаться в IP-адрес кластера Kubernetes. Например, если адрес кластера Kubernetes – 10.80.23.182, FQDN служб должны разрешаться в IP-адрес следующим образом:

    - <console_host>.<smp_domain> – 10.80.23.182
    - <ksc_host>.<smp_domain> – 10.80.23.182
    - <kuma_host>.<smp_domain> – 10.80.23.182

- <api_host>.<smp_domain> – 10.80.23.182
- <monitoring_host>.<smp_domain> – 10.80.23.182

При установке СУБД необходимо также зарезервировать отдельный свободный статический IP-адрес, который будет указан в параметре `pg_ip` и будет использоваться для доступа к PostgreSQL.

13. Создайте учетную запись (например, `sshuser`), которая будет использоваться для развертывания Kaspersky EDR Expert. Эта учетная запись используется для SSH-соединения и должна иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

    a. Выполните следующие команды:

    ```
    # создание пользователя sshuser
    sudo useradd -m -s /bin/bash sshuser
    # создание пароля пользователя sshuser
    sudo passwd sshuser
    # добавление пользователя sshuser в группу sudo
    sudo usermod -aG sudo sshuser
    ```

    b. Откройте файл /etc/sudoers с помощью команды:

    ```
    sudo visudo
    ```

    c. Добавьте следующую строку в конец секции `# Allow members of group sudo to execute any command`:

    ```
    # предоставление привилегий пользователю sshuser для повышения привилегий (sudo) без ввода пароля
    sshuser ALL=(ALL) NOPASSWD: ALL
    ```

    `sshuser` – имя созданного пользователя.

    d. Сохраните и закройте файл /etc/sudoers.

    e. Выполните следующую команду:

    ```
    sudo systemctl restart ssh # restart ssh
    ```

14. Настройте SSH-соединение между устройством администратора и целевыми устройствами:

    a. На устройстве администратора выполните следующую команду, чтобы сгенерировать SSH-ключи с помощью утилиты ssh-keygen без парольной фразы.

    `ssh-keygen -t rsa`

    b. Скопируйте открытый ключ на целевое устройство (например, в директорию `/home/sshuser/.ssh`) с помощью утилиты ssh-copy-id:

    `ssh-copy-id sshuser@<IP_целевого_хоста>`

    Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

    Пример создания открытого ключа

Чтобы создать открытый ключ, выполните следующую команду:

```
ssh-keygen -t rsa
ssh-copy-id sshuser@<IP_целевого_хоста>
```

15. Для корректной работы компонентов Kaspersky EDR Expert откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

16. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

17. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Kaspersky EDR Expert.

    Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации, или конечные сертификаты для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Подготовка устройств к установке сервисов KUMA

Сервисы KUMA (коллекторы, корреляторы и хранилища) устанавливаются на целевые устройства KUMA, расположенные вне кластера Kubernetes.

Доступ к сервисам KUMA выполняется с использованием FQDN целевых устройств KUMA. Устройство администратора должно иметь доступ к целевым устройствам KUMA по своим FQDN.

Если вы планируете использовать несколько тенантов в своей инфраструктуре, создайте отдельный коллектор для каждого тенанта.

Чтобы подготовить целевые устройства KUMA к установке сервисов KUMA:

1. Убедитесь, что выполнены требования к оборудованию, программному обеспечению и установке.

2. Укажите имена устройств.

   Вам нужно указать FQDN, например: kuma1.example.com.

   Не рекомендуется изменять имя устройства KUMA после установки. Это сделает невозможным проверку подлинности сертификатов и нарушит сетевое взаимодействие между компонентами программы.

3. Выполните следующие команды:

   `hostname -f`

   `hostnamectl status`

   Сравните результат команды `hostname -f` и значение поля `Static hostname` в выводе команды `hostnamectl status`. Эти значения должны совпадать с FQDN устройства.

4. Настройте SSH-соединение между устройством администратора и целевыми устройствами KUMA:

   Используйте SSH-ключи, созданные для целевых устройств. Скопируйте открытый ключ на целевые устройства KUMA с помощью утилиты ssh-copy-id.

5. Зарегистрируйте целевые устройства KUMA в зоне DNS вашей организации, чтобы разрешить преобразование имен устройств в IP-адреса.

6. Убедитесь, что на всех целевых устройствах KUMA настроена синхронизация времени по протоколу Network Time Protocol (NTP). Сервисы KUMA (коллекторы, корреляторы и хранилища) устанавливаются на целевые устройства KUMA, расположенные вне кластера Kubernetes.

Устройство готово к установке сервисов KUMA.

Установка системы управления базами данных

Kaspersky EDR Expert поддерживает системы управления базами данных (СУБД) PostgreSQL или Postgres Pro. Полный список поддерживаемых СУБД см. в разделе Аппаратные и программные требования.

Для каждого из следующих компонентов Kaspersky EDR Expert требуется база данных:

- Сервер администрирования
- Платформа автоматизации
- Incident Response Platform (IRP)
- Identity and Access Manager (IAM)

Каждый компонент должен использовать отдельную базу данных в одном экземпляре СУБД. Экземпляр СУБД необходимо устанавливать на отдельном сервере вне кластера Kubernetes. Рекомендуется устанавливать экземпляр СУБД вне кластера Kubernetes.

Для установки СУБД KDT требует наличия привилегированной учетной записи СУБД с правами на создание баз данных и других учетных записей СУБД. KDT использует учетную запись СУБД по умолчанию с правами суперпользователя или другую учетную запись СУБД с такими же правами для создания баз и других учетных записей СУБД, необходимых для компонентов Kaspersky EDR Expert.

Для развертывания на нескольких узлах требуется вручную установить СУБД на отдельном сервере за пределами кластера Kubernetes.

Для развертывания на одном узле вам нужно вручную установить СУБД на целевом устройстве перед развертыванием Kaspersky EDR Expert. В этом случае компоненты СУБД и Kaspersky EDR Expert устанавливаются на одном и том же целевом устройстве, но СУБД не будет включена в кластер Kubernetes.

Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

Пример команды установки PostgreSQL

Для установки PostgreSQL необходимо выполнить следующие команды:

```
sudo apt install -y postgresql-<версия>
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

где `<версия>` – поддерживаемые версии PostgreSQL.

После установки СУБД необходимо настроить параметры сервера СУБД для правильной работы СУБД с Open Single Management Platform.

Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky EDR Expert

Чтобы настроить сервер PostgreSQL или Postgres Pro для работы с Сервером администрирования, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

Kaspersky EDR Expert поддерживает системы управления базами данных (СУБД) PostgreSQL или Postgres Pro. Полный список поддерживаемых СУБД см. в разделе Аппаратные и программные требования. Вы можете настроить параметры сервера СУБД для оптимизации работы СУБД с Сервером администрирования. Соответствие параметров сервера СУБД рекомендуемым значениям является одним из обязательных условий для установки Kaspersky EDR Expert. Соответствие параметров проверяется с помощью KDT.

Найдите конфигурационный файл СУБД:

- Путь по умолчанию к конфигурационному файлу PostgreSQL: `/etc/postgresql/<ВЕРСИЯ>/main/postgresql.conf`
- По умолчанию конфигурационный файл Postgres Pro расположен по пути `/var/lib/pgpro/std-<ВЕРСИЯ>/data/postgresql.conf`

Если конфигурационный файл отсутствует по пути по умолчанию, определите фактическое местоположение файла с помощью следующих команд:

```
sudo su - postgres
psql -c 'SHOW config_file'
```

Вывод команды будет содержать путь к конфигурационному файлу.

Затем выполните следующую команду, чтобы завершить сеанс пользователя `postgres`:

```
exit
```

Рекомендуемые параметры для работы СУБД PostgreSQL и Postgres Pro с Сервером администрирования:

- `listen_addresses = '*'`

  Задает IP-интерфейсы, которые будет прослушивать Сервер администрирования. В целях безопасности настройте сетевой экран, чтобы разрешить доступ к порту 5432 только для доверенных IP-адресов.

- `max_connections = 512`

  Это минимально рекомендованное значение, вы можете указать большее. Если вы используете кластерную СУБД Postgres, укажите параметр `max_connections` для всех серверов СУБД и в конфигурации кластера.

- `shared_buffers = N`

  N = 25%–40% от объема оперативной памяти устройства, на котором установлена СУБД, но не менее 3 ГБ.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth = N`

  Если СУБД установлена на устройстве с операционной системой Linux, N это максимальный размер стека минус запас прочности 1 МБ. Чтобы получить максимальное значение размера стека в КБ, выполните команду "`ulimit -s`".

  Если СУБД установлена на устройстве Windows, оставьте значение по умолчанию 2 МБ.

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = `on`

Если вы используете Postgres Pro 15.7 или Postgres Pro 15.7.1, выключите параметр `enable_compound_index_stats`:

`enable_compound_index_stats = off`

> После обновления конфигурационного файла примените конфигурацию или перезапустите службу СУБД.

Подробную информацию о параметрах сервера PostgreSQL и Postgres Pro, а также о том, как указать эти параметры, см. в документации соответствующей СУБД.

Укажите записи аутентификации для узлов в конфигурационном файле pg_hba.conf. Этот файл находится по тому же пути, что и postgresql.conf.

- В разделе "`# "local" is for Unix domain socket connections only`" для узла `local` в столбце `METHOD` измените значение на `trust`.

- В разделе "`IPv4 local connections`" для узла `host` в столбце `ADDRESS` измените значение на `0.0.0.0/0`.

- Выполните следующую команду, чтобы применить изменения без перезапуска сервера СУБД:

  ```
  sudo -u postgres psql -c "SELECT pg_reload_conf();"
  ```

Укажите пароль пользователя `postgres`.

1. Выполните следующие команды:

   ```
   sudo su - postgres
   psql
   ```

   Вывод команды должен быть следующим:

   ```
   psql (15.12)
   Для получения справки введите "help".
   ```

```
postgres=#
```

2. После `postgres=#` введите `\password`:

```
postgres=# \password
```

3. Введите и повторите пароль:

```
Введите новый пароль для пользователя "postgres".
Введите его еще раз:
```

4. Чтобы завершить сеанс пользователя `postgres`:

```
postgres=# exit
```

Компоненты Kaspersky EDR Expert требуют указания учетных данных суперпользователя PostgreSQL в `parameters.psql_dsn` в качестве `значения`. Укажите учетные данные postgres в конфигурационном файле развертывания. Дополнительные сведения приведены в разделах Развертывание на одном узле: параметры установки и Развертывание на нескольких узлах: параметры установки в зависимости от схемы развертывания.

Проверка подключения к базе данных

Чтобы проверить соединение с базой данных, выполните следующие действия:

1. Убедитесь, что служба Postgres запущена.

```
systemctl list-unit-files | grep postgres
```

Пример вывода:

```
postgrespro-std-17.service                                          enabled         enabled
```

2. Перезапустите службу Postgres:

```
systemctl restart <служба_Postgres>
```

где <`служба_Postgres`> – это имя службы Postgres, полученное на шаге 1 этой инструкции.

3. Запустите `psql`, чтобы проверить подключение:

```
psql -h <fqdn> -U postgres -d postgres
```

Введите пароль, указанный ранее:

```
Пароль для пользователя postgres:
```

Пример вывода:

```
psql (17.4)
Для получения справки введите "help".
```

4. Введите `exit`:

```
postgres=# exit
```

Поддержка кластеров высокой надежности

Высокодоступные кластеры PostgreSQL поддерживаются со следующими параметрами:

- Тип репликации: синхронная.
- Минимальное количество узлов: 3.
- Максимальное количество узлов: 15.

Задайте параметр `psql_dsn` следующим образом: `postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`.

При использовании высокодоступного кластера Postgres версии 14 и выше в качестве базы данных пользователь базы данных должен иметь привилегии `pg_read_all_stats`. Вы можете предоставить эту привилегию, выполнив следующую команду:

```
GRANT pg_read_all_stats TO "dbms_username";
```

где `dbms_username` – имя привилегированной внутренней учетной записи СУБД.

Укажите следующий параметр в конфигурационном файле (`/etc/postgresql/< ВЕРСИЯ >/main/postgresql.conf`):

```
log_hostname = 1
```

Поддержка Corosync/Pacemaker

Чтобы использовать Corosync/Pacemaker, укажите параметр `psql_dsn` с виртуальным IP-адресом кластера СУБД следующим образом:

```
psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
```

Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes

Файл инвентаря KUMA – это файл в формате YAML, который содержит параметры установки для развертывания сервисов KUMA, не включенных в кластер Kubernetes. Путь к файлу инвентаря KUMA включен в конфигурационный файл, который используется Kaspersky Deployment Toolkit для развертывания Kaspersky EDR Expert.

Шаблоны файла инвентаря KUMA находятся в дистрибутиве. Если требуется установить сервисы KUMA (хранилище, коллектор и коррелятор) на одном устройстве, используйте файл single.inventory.yml. Чтобы установить сервисы на нескольких устройствах в сетевой инфраструктуре, используйте файл distributed.inventory.yml.

Рекомендуется создать резервную копию файла инвентаря KUMA, который вы использовали для установки сервисов KUMA. Вы можете использовать его для удаления KUMA.

Чтобы подготовить файл инвентаря KUMA,

откройте шаблон файла инвентаря KUMA, расположенный в дистрибутиве, и измените переменные в файле инвентаря.

Файл инвентаря KUMA содержит следующие секции:

- Секция `all`

  Секция `all` содержит переменные, которые применяются ко всем устройствам, указанным в файле инвентаря. Переменные находятся в секции `vars`.

- Секция `kuma`

  Секция `kuma` содержит переменные, которые применяются к устройствам, на которых будут установлены сервисы KUMA. Эти устройства перечислены в блоке `kuma` в разделе `children`. Переменные находятся в секции `vars`.

В таблице ниже перечислены возможные переменные, их описания, возможные значения и секции файла инвентаря KUMA, в которых могут быть расположены эти переменные.

Список возможных переменных в секции vars

Переменная	Описание	Возможные значения	Секция
Переменные, расположенные в секции `vars` в секциях `all` и `kuma`			
`ansible_connection`	Метод, используемый для подключения к устройствам с сервисами KUMA.	• `ssh` – подключение к целевым устройствам по SSH установлено. • `local` – подключение к целевым устройствам не установлено. Чтобы обеспечить правильную установку сервисов KUMA, в секции `all` установите для переменной `ansible_connection` значение `local`. В секции `kuma` вам нужно указать переменную `ansible_connection` и установить для `ansible_connection` значение `ssh`, чтобы обеспечить подключение к устройствам, на которых установлены сервисы KUMA с помощью SSH.	• `all` • `kuma`
`ansible_user`	Имя пользователя, используемое для подключения к устройствам с сервисами KUMA и для установки внешних сервисов KUMA.	Если пользователь root заблокирован на целевых устройствах, укажите имя пользователя, у которого есть право устанавливать SSH-соединения и повышать привилегии с помощью su или sudo. Чтобы обеспечить правильную установку сервисов KUMA, в секции `all` установите для переменной `ansible_user` значение `nonroot`. В секции `kuma` вам нужно изменить переменную `ansible_user` и указать для переменной `ansible_user` имя пользователя учетной записи, которая может подключаться к удаленным устройствам через SSH, чтобы подготовить их к установке сервисов KUMA.	• `all` • `kuma`
`ansible_become`	Переменная, указывает на необходимость повышения прав учетной записи пользователя, которая используется для установки компонентов KUMA.	• `false` – если значение `ansible_user` – `root`. • `true` – если значение `ansible_user` – не `root`.	`kuma`
`ansible_become_method`	Метод, используемый для повышения привилегий учетной записи пользователя, которая используется для установки компонентов KUMA.	`su` или `sudo`, если значение `ansible_user` не `root`.	`kuma`
Переменные, расположенные в дочернем разделе секции `kuma`			
`kuma_utils`	Группа устройств, на которых хранятся служебные файлы и утилиты KUMA. Устройство может быть включено в группу `kuma_utils` и в группы `kuma_collector`, `kuma_correlator` или `kuma_storage` одновременно. Группа `kuma_utils` может содержать несколько устройств. Во время развертывания Kaspersky EDR Expert на устройствах, входящих в `kuma_utils`, в директорию `/opt/kaspersky/kuma/utils/` копируются следующие файлы: • kuma – исполняемый файл, с которым устанавливаются сервисы KUMA. • LEGAL_NOTICES – файл с информацией о стороннем коде. • kuma-ptvm.tar.gz – это утилита для интеграции с MaxPatrol. • ootb-content – архив с готовыми ресурсами для сервисов KUMA.	Группа устройств содержит переменную `ansible_host`, которая указывает уникальное полное доменное имя устройства и IP-адрес.	`kuma`
`kuma_collector`	Группа устройств коллекторов KUMA. Эта группа может содержать несколько устройств.	Группа устройств коллекторов KUMA содержит переменную `ansible_host`, которая указывает уникальный FQDN устройства и IP-адрес.	`kuma`

`kuma_correlator`	Группа устройств корреляторов KUMA. Эта группа может содержать несколько устройств.	Группа устройств корреляторов KUMA содержит переменную `ansible_host`, которая указывает уникальный FQDN устройства и IP-адрес.	`kuma`
`kuma_storage`	Группа устройств хранилищ KUMA. Эта группа может содержать несколько устройств.	Группа устройств хранилищ KUMA содержит переменную `ansible_host`, которая указывает уникальный FQDN устройства и IP-адрес.	`kuma`

Пример шаблона файла инвентаря KUMA для установки сервисов KUMA на отдельном устройстве (файл single.inventory.yml)

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 1
```

Пример шаблона файла инвентаря KUMA для установки сервисов KUMA на нескольких устройствах (файл distributed.inventory.yml)

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma-utils.example.com:
        ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
```

```
      kuma-collector-1.example.com:
      ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
      kuma-correlator-1.example.com:
      ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
      kuma-storage-1.example.com:
          ansible_host: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 1
      kuma-storage-2.example.com:
          ansible_host: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 2
      kuma-storage-3.example.com:
          ansible_host: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 3
      kuma-storage-4.example.com:
          ansible_host: 0.0.0.0
          shard: 2
          replica: 2
```

Развертывание на нескольких узлах: параметры установки

Конфигурационный файл – это файл в формате YAML, содержащий набор параметров установки компонентов Kaspersky EDR Expert.

> Параметры установки, указанные в таблицах ниже, необходимы для развертывания на нескольких узлах Kaspersky EDR Expert. Чтобы развернуть Kaspersky EDR Expert на отдельном узле, используйте конфигурационный файл, содержащий параметры установки, характерные для развертывания на одном узле.

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT. Вы можете заполнить шаблон конфигурационного файла вручную либо вы можете использовать мастер развертывания, чтобы указать параметры установки, необходимые для развертывания Kaspersky EDR Expert, и сгенерировать конфигурационный файл.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны перед развертыванием Kaspersky EDR Expert. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения. Значения параметров должны соответствовать описанным ниже правилам. Во время развертывания Kaspersky EDR Expert, KDT проверяет, правильно ли указаны нужные параметры установки. Если необходимые параметры в конфигурационном файле отсутствуют или недействительны, развертывание будет прервано.

Пример конфигурационного файла развертывания Kaspersky EDR Expert на нескольких узлах

```
schemaType: ParameterSet
```

```
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Nodes on which the Kubernetes cluster and Kaspersky EDR will be deployed
nodes:
  # Параметры управляющего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-primary1
    # Тип узла.
    # Возможные типы узлов: управляющий, рабочий.
    # Управляющий узел предназначен для управления кластером, хранения метаданных и
    распределения рабочей нагрузки.
    type: primary
    # IP-адрес узла.
    # Управляющий и рабочие узлы должны быть включены в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.42
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
  # Параметры рабочего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-w1
    # Тип узла.
    # Возможные типы узлов: управляющий, рабочий.
    # The workload of Kaspersky EDR components is distributed between worker nodes.
    type: worker
    # Служба KUMA будет установлена на рабочем узле. Можно указать один или несколько
    служб KUMA либо не указывать их вообще.
    kuma_roles: ["core","metrics","collector"]
    # IP-адрес узла.
    # Управляющий и рабочие узлы должны быть включены в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.141
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
  # Параметры рабочего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
```

```
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-w2
    # Тип узла.
    # Возможные типы узлов: управляющий, рабочий.
    # The workload of Kaspersky EDR components is distributed between worker nodes.
    type: worker
    # IP-адрес узла.
    # Первичный и рабочие узлы должны быть включены в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.45
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
  # Параметры рабочего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-w3
    # Тип узла.
    # Возможные типы узлов: управляющий, рабочий.
    # The workload of Kaspersky EDR components is distributed between worker nodes.
    type: worker
    # IP-адрес узла.
    # Первичный и рабочие узлы должны быть включены в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.30
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
# Parameters for the Kaspersky EDR deployment
parameters:
  # Строка подключения для доступа к СУБД, которая установлена и настроена на отдельном
  сервере.
  # user_db – имя пользователя привилегированной внутренней учетной записи СУБД. Этой
  учетной записи предоставлены права на создание баз данных и других учетных записей
  СУБД.
  # password_db – пароль привилегированной внутренней учетной записи СУБД.
  # fqdn_db:port_db – полное имя домена и порт подключения отдельного сервера, на котором
  установлена СУБД.
  # Значение параметра 'psql_dsn' должно соответствовать URI-формату. Если URI-
  подключение включает специальные символы в любой из его частей, символы должны быть
  экранированы с помощью процентной кодировки.
  - name: psql_dsn
```

```
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# IP-адрес шлюза кластера Kubernetes.
# The Kubernetes cluster gateway is intended for connecting to the Kaspersky EDR
components installed inside the Kubernetes cluster.
# Шлюз кластера должен быть включен в ту же подсеть, что и все узлы кластера.
- name: ingress_ip
  source:
    value: 10.80.23.182
# Путь к закрытой части SSH-ключа для подключения к управляющему и рабочим узлам с
помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky EDR user account that will be created during the
installation.
# Длина пароля должна быть от 10 до 256 символов.
# Он может содержать строчные или прописные буквы (a–z; A–Z), цифры (0–9) и специальные
символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
# Пароль не должен содержать пробелы или сочетания символов ".@".
- name: admin_password
  source:
    value: "password"
# Количество дискового пространства для работы Ядра KUMA, в гигабайтах.
# Указано как "<amount>Gi". По умолчанию указано значение 512Gi.
# Если параметр 'low_resources' установлен в значение true, параметр
'core_disk_request' игнорируется и выделяется 4Gi.
- name: core_disk_request
  source:
    value: 512Gi
# Путь к файлу инвентаря KUMA, который содержит параметры установки для развертывания
сервисов KUMA. Этот файл расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Путь к лицензионному ключу Kaspersky Endpoint Detection and Response. Этот файл
расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: license
  source:
    value: "/home/user/license.key"
# Имя домена. Значение параметра должно соответствовать требованиям назначения имен
доменов до четвертого уровня.
# The service host name and domain name are parts of FQDNs of the Kaspersky EDR
services.
# Значения по умолчанию для имен служб устройств: nwc_host—"console", flow_host
—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host
—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Пользовательские имена устройств могут быть указаны в конфигурационном файле.
# Пример: console.smp.local является FQDN службы, предоставляющей доступ к Консоли
OSMP. Этот FQDN состоит из значений параметров 'console_host' и 'smp_domain'.
- name: smp_domain
  source:
```

```
    value: "smp.local"
# List of host names of the Kaspersky EDR services for which a self-signed or custom
certificate must be generated.
# Значение параметра должно быть списком имен устройств, разделенных пробелами. Если
пользовательские имена устройств не указаны, используются имена устройств по умолчанию:
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина имени пользователя должна быть от 1 до 30 символов.
# Имя пользователя может содержать строчные буквы (от 'a' до 'z'), цифры (от '0' до
'9') и специальные символы (_ - .).
# Имя пользователя должно начинаться с буквы и не должно содержать пробелы или символ
"@".
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина пароля должна быть от 8 до 256 символов.
# Он может содержать строчные или прописные буквы (a–z; A–Z), цифры (0–9) и специальные
символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Раздел `nodes` конфигурационного файла содержит параметры установки для каждого целевого устройства кластера Kubernetes. Эти параметры перечислены в таблице ниже.

Раздел nodes

Имя параметра	Обязательная	Описание

`desc`	Да	Имя узла.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Все узлы кластера должны иметь уникальные имена. Это требование является одним из обязательных для установки Kaspersky EDR Expert и проверяется с помощью KDT.

`type`	Да	Тип узла. Возможные значения параметра: • `primary` • `worker` • `loadbalancer`

Имя параметра	Обязательная	Описание
`host`	Да	IP-адрес узла. Все узлы должны быть включены в ту же подсеть, что и шлюз кластера Kubernetes. Для узлов требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера. При наличии нескольких управляющих узлов вам потребуется балансировщик нагрузки для распределения поступающих запросов по управляющим узлам и обеспечения равномерной рабочей нагрузки. Если вы хотите использовать внешний балансировщик нагрузки, выделите отдельное устройство вне кластера и укажите его параметры в файле конфигурации. Если вы не хотите использовать внешний балансировщик нагрузки, его роль будут выполнять рабочие узлы.
`kuma_role`	Нет	Служба KUMA, которую вы можете указать для установки на рабочем узле. Можете задать установку одного или нескольких служб KUMA, либо не указывать их установку. Параметр `kuma_roles` учитывается при установке службы KUMA в кластере Kubernetes с помощью Консоли OSMP. Если узел, на котором вы планируете установить службу KUMA, перегружен, кластер выберет другой, менее загруженный узел для установки службы. Для параметра `inventory` установите значение `/dev/null`. Хранилища, созданные из одного ресурса KUMA, не разрешается размещать на одном рабочем узле. Данное правило добавлено для обеспечения необходимого уровня отказоустойчивости. Возможные значения параметра: • `core` – ядро KUMA • `metrics` – просмотр метрик KUMA • `collector` – коллектор • `correlator` – коррелятор • `storage` – хранилище Значение параметра указывается в виде списка строк, включающих в себя роли KUMA. Например: `kuma_roles: ["core","metrics","collector"]`

`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 31 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • нижнее подчеркивание (_), дефис (-).

`password`	Нет	Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного в параметре `ssh_pk`.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Имя параметра	Обязательная	Описание
psql_dsn	Да	Строка подключения для доступа к СУБД, которая установлена и настроена вне кластера Kubernetes. Укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port> где: • dbms_username – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Kaspersky EDR Expert. • password – пароль привилегированной внутренней учетной записи СУБД. • fqdn:port – полное имя домена и порт подключения целевого устройства, на котором установлена СУБД. Чтобы использовать кластер высокой доступности, укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port> Чтобы использовать Corosync/Pacemaker, укажите этот параметр с виртуальным IP-адресом следующим образом: psql_dsn=postgres://postgres:pass!@<virtual ip>:<port> Значение параметра psql_dsn должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки. Символы, которые требуется заменить в значении параметра psql_dsn: • Пробел → %20 • ! → %21 • # → %23 • % → %25 • & → %26 • / → %2F • : → %3A • = → %3D • ? → %3F • @ → %40 • [→ %5B •] → %5D Дополнительную информацию см. в статье Строка подключения PostgreSQL.
nwc-language	Да	Язык интерфейса OSMP Console, указанный по умолчанию. После установки вы можете изменить язык OSMP Console. Возможные значения параметра: • enUS (значение по умолчанию) • ruRu Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
ingress_ip	Да	Зарезервированный статический IPv4-адрес шлюза кластера Kubernetes. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Шлюз кластера должен быть включен в ту же подсеть, что управляющий и рабочие узлы кластера.
ssh_pk	Да	Путь к закрытой части SSH-ключа, которая находится на устройстве администратора и используется для подключения к управляющему рабочему узлу и к узлам со службами KUMA (коллекторам, корреляторам и хранилищам) с помощью утилиты KDT. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.

Имя параметра	Обязательная	Описание
`admin_password`	Да	Параметр `admin_password` задает пароль Kaspersky EDR Expert, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 10 или более 256 символов. • Пароль должен содержать символы как минимум трех групп из списка ниже: • верхний регистр (A–Z); • нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;). • Пароль не должен содержать пробелов или комбинации ".@". Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера развертывания), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Нет	Параметр, указывающий на то, что приложение Kaspersky EDR Expert установлено на целевом устройстве с ограниченными вычислительными ресурсами. В случае развертывания на нескольких узлах установите для параметра `low_resources` значение `false`. Возможные значения параметра: • `true` – установка с ограниченными вычислительными ресурсами (для развертывания на одном узле). • `false` – стандартная установка (значение по умолчанию).
`core_disk_request`	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `false` или ничего не указано, для работы Ядра KUMA будет выделен объем дискового пространства 100 ГБ по умолчанию. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `true`, для работы Ядра KUMA будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр `core_disk_request` позже, после развертывания приложения.
`metrics_disk_request`	Да	Параметр, задающий объем дискового пространства для работы службы Метрики. Если параметр `metrics_disk_request` не задан, а для параметра `low_resources` установлено значение `false` или не установлено значение, для работы службы Метрики будет выделен объем дискового пространства 80 ГБ по умолчанию. Если параметр `metrics_disk_request` не задан, а для параметра `low_resources` установлено значение `true`, для работы службы Метрики будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр `metrics_disk_request` позже, после развертывания приложения.
`inventory`	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если все сервисы KUMA будут установлены внутри кластера, для параметра `inventory` установите значение `/dev/null`.

Имя параметра	Обязательная	Описание
`host_inventory`	Нет	Путь к дополнительному файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если вы выполняете первоначальное развертывание Kaspersky EDR Expert или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (`/dev/null`).
`license`	Нет	Путь к KUMA лицензионному ключу, находящемуся на устройстве администратора. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Вы можете загрузить лицензионный ключ или указать код активации при входе в OSMP после завершения развертывания.

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
`xdr_edr_ingress_host`
	Да	Имя устройства, которое используется в FQDN публичных служб Kaspersky EDR Expert. Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.
		Если пользовательские имена устройств не указаны, используются следующие имена устройств по умолчанию:
		• `nwc_host – "console"`
		• `flow_host – "console"`
		• `hydra_host – "console"`
		• `login_host – "console"`
		• `ksc_host–"admsrv"`
		• `console_host – "console"`
		• `api_host – "api"`
		• `kuma_host – "kuma"`
		• `monitoring_host – "monitoring"`
		• `xdr_edr_ingress_host–"agentserver"`

`smp_domain`	Да	Имя домена, которое используется в FQDN публичных служб Kaspersky EDR Expert. Значение параметра должно соответствовать требованиям назначения имен доменов до четвертого уровня. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.
`pki_host_list`	Да	Список имен устройств публичных служб Kaspersky EDR Expert, для которых требуется сформировать самоподписанный или пользовательский сертификат. Значение параметра должно быть списком имен устройств разделенных пробелами.
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Kaspersky EDR Expert. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат. • `false` – использовать самоподписанные сертификаты (значение по умолчанию).
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, который используется для работы с общедоступными службами Kaspersky EDR Expert. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.

Имя параметра	Обязательная	Описание

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с соответствующими публичными службами Kaspersky EDR Expert: `<admsrv_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<kuma_host>.<smp_domain>`, `<monitoring_host>.<smp_domain>` и `<console_host>.<smp_domain>`. Значения параметров должны быть Linux-путем к файлу или содержимым файла в кодировке Base64.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметры `intermediate_bundle` и `pki_host_list`.

`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных). Измеряется в гигабайтах, указывается как "<объем>Gi". Требуемый объем свободного места на диске зависит от количества управляемых устройств и других параметров и может быть рассчитан. Значение по умолчанию – 30 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Измеряется в гигабайтах, указывается как "<объем>GB". Минимальное рекомендуемое значение и значение по умолчанию – 5 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.

`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 30 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (_ - .)
		• Имя пользователя должно начинаться с буквы.
		• Имя пользователя не должно содержать пробелов или символа "@".

`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Пароль должен соответствовать следующим правилам:
		• Пароль пользователя не может содержать менее 8 или более 256 символов.
		• Пароль должен содержать символы из указанных ниже групп:
		  • верхний регистр (A–Z);
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Измеряется в гигабайтах, указывается как " <объем>Gi". Минимальное рекомендуемое значение и значение по умолчанию – 40 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. По умолчанию указано значение 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h"). Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.

Имя параметра	Обязательная	Описание
psql_tls_off	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Kaspersky EDR Expert и СУБД по протоколу TLS. Если СУБД установлена за пределами кластера, шифрование TLS выключено по умолчанию (значение по умолчанию true). Возможные значения параметра: • true – трафик не шифруется (значение по умолчанию). • false – трафик шифруется.
psql_trusted_cas	Нет	Путь к PEM-файлу, который может содержать TLS-сертификат сервера СУБД или корневой сертификат, из которого может быть выдан сертификат TLS-сервера. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Укажите параметр psql_trusted_cas, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра psql_tls_off указано значение false).
proxy_enabled	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Kaspersky EDR Expert к интернету. Если устройство, на котором установлен Kaspersky EDR Expert, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Kaspersky EDR Expert (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. Возможные значения параметра: • true – использовать прокси-сервер. • false – не использовать прокси-сервер (значение по умолчанию).
proxy_addresses	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "0.0.0.0 0.0.0.1 0.0.0.2"). Укажите этот параметр, если для параметра proxy_enabled указано значение true.
proxy_port	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра proxy_enabled указано значение true.
console_port	Нет	Параметр, который указывает настраиваемый номер порта для подключения к серверу Консоли OSMP. По умолчанию: 443
as_smp_port	Нет	Параметр, указывающий настраиваемый номер порта, используемого Endpoint Agents для подключения к компоненту agentserver. По умолчанию: 443
kuma_gateway_telemetry_listener_port	Нет	Параметр, указывающий пользовательский номер порта, используемого для отправки телеметрии. По умолчанию указано значение 443.
trace_level	Нет	Уровень детализации файлов трассировки Сервера администрирования. Трассировка записывается во время работы Сервера администрирования. Значение по умолчанию – 0, трассировка не записывается. Возможные значения параметра: 0–5. Чем выше значение параметра, тем более подробная информация о трассировке записывается.
ansible_extra_flags	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • -v • -vv • -vvv • -vvvv По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.
incident_attachments_max_count_limit	Нет	Количество файлов, которые вы можете прикрепить к инциденту. По умолчанию указано значение 100.

Имя параметра	Обязательная	Описание
`incident_attachments_max_size_limit`	Нет	Общий размер файлов, прикрепленных к инциденту. Измеряется в байтах. Единицы измерения не отображаются. По умолчанию указано значение `26214400`.
`ignore_precheck`	Нет	Параметр, указывающий, следует ли проверить аппаратное и программное обеспечение, а также конфигурацию сети узлов кластера Kubernetes на соответствие требованиям, необходимым для установки решения перед развертыванием. Возможные значения параметра: • `true` – пропустить предварительные проверки. • `false` – выполнить предварительные проверки (значение по умолчанию).
`airgap_mode`	Нет	Параметр, включающий или выключающий предварительную проверку и обновление кеша пакетов пакетным менеджером APT. Таким образом становится возможным развертывание Kaspersky EDR Expert в среде с физической изоляцией. Возможные значения параметра: • `true` – пропустить предварительную проверку и обновление кеша пакетов. • `false` – выполнить предварительную проверку и обновление кеша пакетов (значение по умолчанию).
`grafana_smtp_host`	Нет	Адрес SMTP-сервера для Grafana, который используется для отправки уведомлений о событиях, связанных с работоспособностью кластера Kubernetes, по электронной почте. Укажите этот параметр в формате `<хост>:<порт>` – например, `localhost:25`.
`grafana_smtp_user`	Нет	Имя пользователя для аутентификации на SMTP-сервере.
`grafana_smtp_password`	Нет	Пароль для аутентификации на SMTP-сервере.
`grafana_smtp_bundle`	Нет	Файл, содержащий цепочку сертификатов X.509, которая используется для проверки TLS-подключения к SMTP-серверу.
`grafana_smtp_skip_verify`	Нет	Данный параметр указывает, следует ли пропускать проверку TLS-сертификата для SMTP-сервера. Возможные значения параметра: • `true` – пропустить проверку TLS-сертификата. • `false` – выполнять проверку TLS-сертификата (значение по умолчанию).
`grafana_smtp_from_address`	Нет	Электронный адрес отправителя, который будет отображаться в поле "От" при отправке уведомлений по электронной почте.
`grafana_smtp_from_name`	Нет	Отображаемое имя отправителя в уведомлениях по электронной почте.
`grafana_smtp_ehlo_identity`	Нет	Идентификатор, используемый в команде EHLO при подключении к SMTP-серверу.
`grafana_starttls_policy`	Нет	Политика использования STARTTLS при подключении к SMTP-серверу. Возможные значения параметра: • `OpportunisticStartTLS` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования. • `MandatoryStartTLS` – требовать STARTTLS и завершаться с ошибкой, если SMTP-сервер не поддерживает STARTTLS. • `NoStartTLS` – не использовать STARTTLS и подключиться к SMPT-серверу без шифрования. • `empty` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования (значение по умолчанию).
`grafana_smtp_enable_tracing`	Нет	Параметр, который указывает, следует ли включить ли трассировку SMTP-подключения для отладки отправки электронной почты. Возможные значения параметра: • `true` – включить трассировку SMTP-подключения. • `false` – отключить трассировку SMTP-подключения (значение по умолчанию).

Имя параметра	Обязательная	Описание
autodeploy_plan	Нет	Параметр, указывающий, следует ли развертывать сервисы KUMA для Kaspersky EDR или для Kaspersky NGFW. Возможные значения параметра: • edr – развернуть службы KUMA для OSMP и Kaspersky EDR в кластере Kubernetes (значение по умолчанию). • ngfw – развернуть службы KUMA для OSMP и Kaspersky NGFW внутри кластера Kubernetes. Также предустановленный коллектор **[OOTB] Kaspersky NGFW** будет установлен на первом устройстве из списка устройств, указанного в параметре kuma_collector файла инвентаря KUMA. • none – не разворачивать службы KUMA для Kaspersky EDR или Kaspersky NGFW. Это значение следует указывать при развертывании Kaspersky EDR Expert без сервисов KUMA для Kaspersky EDR и Kaspersky NGFW или при восстановлении Kaspersky EDR Expert из резервной копии. Если при восстановлении Kaspersky EDR Expert задать значения edr или ngfw, это может привести к конфликту между развернутыми сервисами и сервисами из резервной копии.
tokenhub_access_token	Нет	Время жизни токена доступа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "1h10m" или "2h". Минимальное значение – 5m, а максимальное значение – 2h. Значение по умолчанию – 1h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр tokenhub_access_token позже, после развертывания приложения.
tokenhub_refresh_token	Нет	Время жизни токена обновления, используемого для получения нового токена доступа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1240h30m". Минимальное значение – 12m, а максимальное значение – 4320h. Значение по умолчанию – 24h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр tokenhub_refresh_token позже, после развертывания приложения.
credentials_session_ttl	Нет	Максимальное время простоя сеанса единого входа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1h30m". Минимальное значение – 5m, а максимальное значение – 96h. Значение по умолчанию – 1h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр credentials_session_ttl позже, после развертывания приложения.

Развертывание на одном узле: параметры установки

Конфигурационный файл, используемый для развертывания Kaspersky EDR Expert на одном узле, содержит параметры установки, необходимые как для развертывания на нескольких узлах, так и для развертывания на одном узле. Также этот конфигурационный файл содержит параметры, специфичные для развертывания на одном узле (openbao_ha_mode, openbao_standalone и default_class_replica_count).

Шаблон конфигурационного файла (singlenode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT. Вы можете заполнить шаблон конфигурационного файла вручную либо вы можете использовать мастер развертывания, чтобы указать параметры установки, необходимые для развертывания Kaspersky EDR Expert, и сгенерировать конфигурационный файл.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны перед развертыванием Kaspersky EDR Expert. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения. Значения параметров должны соответствовать описанным ниже правилам. Во время развертывания Kaspersky EDR Expert, KDT проверяет, правильно ли указаны нужные параметры установки. Если необходимые параметры в конфигурационном файле отсутствуют или недействительны, развертывание будет прервано.

Пример конфигурационного файла для развертывания Kaspersky EDR Expert на одном узле

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky EDR will be deployed
nodes:
  # Параметры управляющего рабочего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-1
    # Тип узла.
    # Для развертывания на одном узле установите для параметра "type" значение "primary-
    worker". В этом случае целевое устройство будет действовать как управляющий и рабочий
    узлы.
    type: primary-worker
    # IP-адрес узла.
    # Управляющий рабочий узел должен быть включен в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.42
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
# Parameters for the Kaspersky EDR deployment
parameters:
  # Строка подключения для доступа к СУБД, которая установлена и настроена на отдельном
  сервере.
  # user_db – имя пользователя привилегированной внутренней учетной записи СУБД. Этой
  учетной записи предоставлены права на создание баз данных и других учетных записей
  СУБД.
  # password_db – пароль привилегированной внутренней учетной записи СУБД.
  # fqdn_db:port_db – полное имя домена и порт подключения отдельного сервера, на котором
  установлена СУБД.
```

```
# Значение параметра 'psql_dsn' должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.
- name: psql_dsn
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# IP-адрес шлюза кластера Kubernetes.
# The Kubernetes cluster gateway is intended for connecting to the Kaspersky EDR components installed inside the Kubernetes cluster.
# Шлюз кластера должен быть включен в ту же подсеть, что и управляющий рабочий узел кластера.
- name: ingress_ip
  source:
    value: 10.80.23.182
# Путь к закрытой части SSH-ключа для подключения к управляющему рабочему узлу с помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky EDR user account that will be created during the installation.
# Длина пароля должна быть от 10 до 256 символов.
# Он может содержать строчные или прописные буквы (a–z; A–Z), цифры (0–9) и специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
# Пароль не должен содержать пробелы или сочетания символов ".@".
- name: admin_password
  source:
    value: ""
# The parameter indicating that Kaspersky EDR is installed on the target host with limited computing resources.
# For the single-node deployment, set the 'low_resources' parameter to "true" so that Kaspersky Symphony EDR components will require less memory and CPU resources.
# Если вы включите этот параметр, для установки Ядра KUMA на целевом устройстве будет выделено 4 ГБ свободного дискового пространства.
- name: low_resources
  source:
    value: "true"
# The number of disk volumes that are used to store the service data of Kaspersky EDR components and KDT.
# Для развертывания на одном узле установите для параметра значение "1".
- name: default_class_replica_count
  source:
    value: "1"
# Параметр, который указывает, следует ли запускать хранилище секретов в режиме High Availability (HA).
# Для развертывания на одном узле установите для параметра значение "false".
- name: openbao_ha_mode
  source:
    value: "false"
# Параметр, который указывает, следует ли запускать хранилище секретов в автономном режиме.
# Для развертывания на одном узле установите для параметра значение "true".
- name: openbao_standalone
  source:
    value: "true"
```

```
# Путь к файлу инвентаря KUMA, который содержит параметры установки для развертывания
сервисов KUMA. Этот файл расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Путь к лицензионному ключу Kaspersky Endpoint Detection and Response. Этот файл
расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: license
  source:
    value: "/home/user/license.key"
# Имя домена. Значение параметра должно соответствовать требованиям назначения имен
доменов второго уровня.
# The service host name and domain name are parts of FQDNs of the Kaspersky EDR
services.
# Значения по умолчанию для имен служб устройств: nwc_host—"console", flow_host
—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host
—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Пользовательские имена устройств могут быть указаны в конфигурационном файле.
# Пример: console.smp.local является FQDN службы, предоставляющей доступ к Консоли
OSMP. Этот FQDN состоит из значений параметров 'console_host' и 'smp_domain'.
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky EDR services for which a self-signed or custom
certificate must be generated.
# Значение параметра должно быть списком имен устройств, разделенных пробелами. Если
пользовательские имена устройств не указаны, используются имена устройств по умолчанию:
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина имени пользователя должна быть от 1 до 30 символов.
# Имя пользователя может содержать строчные буквы (от 'a' до 'z'), цифры (от '0' до
'9') и специальные символы (_ - .).
# Имя пользователя должно начинаться с буквы и не должно содержать пробелы или символ
"@".
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина пароля должна быть от 8 до 256 символов.
# Он может содержать строчные или прописные буквы (a–z; A–Z), цифры (0–9) и специальные
символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Раздел `nodes` конфигурационного файла содержит параметры целевого устройства, которые перечислены в таблице ниже.

Раздел nodes

Имя параметра	Обязательная	Описание

`desc`	Да	Имя узла.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Все узлы кластера должны иметь уникальные имена. Это требование является одним из обязательных для установки Kaspersky EDR Expert и проверяется с помощью KDT.

`type`	Да	Тип узла. Для целевого устройства для параметра `type` задайте значение `primary-worker`, чтобы включить **развертывание на одном узле**. В этом случае целевое устройство будет действовать как первичный и рабочий узлы.
`host`	Да	IP-адрес узла. Управляющий рабочий узел должен быть включен в ту же подсеть, что и шлюз кластера Kubernetes. Для узла требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера.
`kuma_role`	Нет	Сервис KUMA, который вы можете указать для установки на рабочем узле. Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на рабочих узлах, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его. Если все сервисы KUMA будут установлены внутри кластера, для параметра `inventory` установите значение `/dev/null`. Для **развертывания на одном узле** оставьте этот параметр пустым, так как все сервисы будут установлены на одном узле.

`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 31 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • нижнее подчеркивание (_), дефис (-).

`password`	Нет	Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного в параметре `ssh_pk`.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Имя параметра	Обязательная	Описание
psql_dsn	Да	Строка подключения для доступа к СУБД, которая установлена и настроена вне кластера Kubernetes. Укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port> где: • dbms_username – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Kaspersky EDR Expert. • password – пароль привилегированной внутренней учетной записи СУБД. • fqdn:port – полное имя домена и порт подключения целевого устройства, на котором установлена СУБД. Если ваша СУБД установлена на том же узле, что и узел кластера Kubernetes, не используйте localhost или 127.0.0.1 в качестве адреса сервера СУБД в параметре psql_dsn. Используйте IP-адрес устройства, доступный по сети кластера (не loopback-адрес). Чтобы использовать кластер высокой доступности, укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port> Чтобы использовать Corosync/Pacemaker, укажите этот параметр с виртуальным IP-адресом следующим образом: psql_dsn=postgres://postgres:pass!@<virtual ip>:<port> Значение параметра psql_dsn должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки. Символы, которые требуется заменить в значении параметра psql_dsn: • Пробел → %20 • ! → %21 • # → %23 • % → %25 • & → %26 • / → %2F • : → %3A • = → %3D • ? → %3F • @ → %40 • [→ %5B •] → %5D Дополнительную информацию см. в статье Строка подключения PostgreSQL.
nwc-language	Да	Язык интерфейса OSMP Console, указанный по умолчанию. После установки вы можете изменить язык OSMP Console. Возможные значения параметра: • enUS (значение по умолчанию) • ruRu Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
ingress_ip	Да	Зарезервированный статический IPv4-адрес шлюза кластера Kubernetes. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Шлюз кластера должен быть включен в ту же подсеть, что и первичный рабочий узел кластера. Для шлюза кластера Kubernetes требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера. В качестве значения этого параметра нельзя указывать IP-адрес того же устройства, на котором выполняется развертывание.

Имя параметра	Обязательная	Описание
`ssh_pk`	Да	Путь к закрытой части SSH-ключа, которая находится на устройстве администратора и используется для подключения к управляющему рабочему узлу и к узлам со службами KUMA (коллекторам, корреляторам и хранилищам) с помощью утилиты KDT. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.
`admin_password`	Да	Параметр `admin_password` задает пароль Kaspersky EDR Expert, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 10 или более 256 символов. • Пароль должен содержать символы как минимум трех групп из списка ниже: • верхний регистр (A–Z); • нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;). • Пароль не должен содержать пробелов или комбинации ".@". Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера развертывания), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Да	Параметр, указывающий, что Kaspersky EDR Expert установлен на целевом устройстве с ограниченными вычислительными ресурсами. Возможные значения параметра: • `true` – установка с ограниченными вычислительными ресурсами (для развертывания на одном узле). • `false` – стандартная установка. Для **развертывания на одном узле** установите для параметра `low_resources` значение `true`, чтобы компоненты Kaspersky EDR Expert требовали меньше ресурсов памяти и процессора. Если вы включите этот параметр, для установки Ядра KUMA на целевом устройстве будет выделено 4 ГБ свободного дискового пространства.
`openbao_ha_mode`	Да	Параметр, который указывает, следует ли запускать хранилище секретов в режиме High Availability (HA). Возможные значения параметра: • `true` • `false` Для **развертывания на одном узле** установите для параметра `openbao_ha_mode` значение `false`.
`openbao_standalone`	Да	Параметр, который указывает, следует ли запускать хранилище секретов в автономном режиме. Возможные значения параметра: • `true` • `false` Для **развертывания на одном узле** установите для параметра `openbao_standalone` значение `true`.
`default_class_replica_count`	Да	Количество дисковых томов, на которых хранятся служебные данные компонентов Kaspersky EDR Expert и KDT. По умолчанию указано значение `3`. Для **развертывания на одном узле** установите для параметра `default_class_replica_count` значение `1`.

Имя параметра	Обязательная	Описание
`core_disk_request`	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `false` или ничего не указано, для работы Ядра KUMA будет выделен объем дискового пространства 100 ГБ по умолчанию. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `true`, для работы Ядра KUMA будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр `core_disk_request` позже, после развертывания приложения.
`inventory`	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если все сервисы KUMA будут установлены внутри кластера, для параметра `inventory` установите значение `/dev/null`.
`host_inventory`	Нет	Путь к дополнительному файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если вы выполняете первоначальное развертывание Kaspersky EDR Expert или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (`/dev/null`).
`license`	Нет	Путь к KUMA лицензионному ключу, находящемуся на устройстве администратора. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Вы можете загрузить лицензионный ключ или указать код активации при входе в OSMP после завершения развертывания.

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
`xdr_edr_ingress_host`
	Да	Имя устройства, которое используется в FQDN публичных служб Kaspersky EDR Expert. Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.
		Если пользовательские имена устройств не указаны, используются следующие имена устройств по умолчанию:
		• `nwc_host – "console"`
		• `flow_host – "console"`
		• `hydra_host – "console"`
		• `login_host – "console"`
		• `ksc_host–"admsrv"`
		• `console_host – "console"`
		• `api_host – "api"`
		• `kuma_host – "kuma"`
		• `monitoring_host – "monitoring"`
		• `xdr_edr_ingress_host–"agentserver"`

`smp_domain`	Да	Имя домена, которое используется в FQDN публичных служб Kaspersky EDR Expert. Значение параметра должно соответствовать требованиям назначения имен доменов до четвертого уровня. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.
`pki_host_list`	Да	Список имен устройств публичных служб Kaspersky EDR Expert, для которых требуется сформировать самоподписанный или пользовательский сертификат. Значение параметра должно быть списком имен устройств разделенных пробелами.

Имя параметра	Обязательная	Описание
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Kaspersky EDR Expert. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат. • `false` – использовать самоподписанные сертификаты (значение по умолчанию).
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, который используется для работы с общедоступными службами Kaspersky EDR Expert. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с соответствующими публичными службами Kaspersky EDR Expert: `<admsrv_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<kuma_host>.<smp_domain>`, `<monitoring_host>.<smp_domain>` и `<console_host>.<smp_domain>`. Значения параметров должны быть Linux-путем к файлу или содержимым файла в кодировке Base64.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметры `intermediate_bundle` и `pki_host_list`.

`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных). Измеряется в гигабайтах, указывается как "<объем>Gi". Требуемый объем свободного места на диске зависит от количества управляемых устройств и других параметров и может быть рассчитан. Значение по умолчанию – 30 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Измеряется в гигабайтах, указывается как "<объем>GB". Минимальное рекомендуемое значение и значение по умолчанию – 5 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.

`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 30 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (_ - .)
		• Имя пользователя должно начинаться с буквы.
		• Имя пользователя не должно содержать пробелов или символа "@".

`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Пароль должен соответствовать следующим правилам:
		• Пароль пользователя не может содержать менее 8 или более 256 символов.
		• Пароль должен содержать символы из указанных ниже групп:
		  • верхний регистр (A–Z);
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

Имя параметра	Обязательная	Описание
`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение и значение по умолчанию – 40 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. По умолчанию указано значение 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h"). Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.
`psql_tls_off`	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Kaspersky EDR Expert и СУБД по протоколу TLS. Если СУБД установлена за пределами кластера, шифрование TLS выключено по умолчанию (значение по умолчанию `true`). Возможные значения параметра: • `true` – трафик не шифруется (значение по умолчанию). • `false` – трафик шифруется.
`psql_trusted_cas`	Нет	Путь к PEM-файлу, который может содержать TLS-сертификат сервера СУБД или корневой сертификат, из которого может быть выдан сертификат TLS-сервера. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Укажите параметр `psql_trusted_cas`, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра `psql_tls_off` указано значение `false`).
`proxy_enabled`	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Kaspersky EDR Expert к интернету. Если устройство, на котором установлен Kaspersky EDR Expert, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Kaspersky EDR Expert (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. Возможные значения параметра: • `true` – использовать прокси-сервер. • `false` – не использовать прокси-сервер (значение по умолчанию).
`proxy_addresses`	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "`0.0.0.0 0.0.0.1 0.0.0.2`"). Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`proxy_port`	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`console_port`	Нет	Параметр, который указывает настраиваемый номер порта для подключения к серверу Консоли OSMP. По умолчанию: 443
`as_smp_port`	Нет	Параметр, указывающий настраиваемый номер порта, используемого Endpoint Agents для подключения к компоненту agentserver. По умолчанию: 443
`kuma_gateway_telemetry_listener_port`	Нет	Параметр, указывающий пользовательский номер порта, используемого для отправки телеметрии. По умолчанию указано значение 443.

Имя параметра	Обязательная	Описание
`trace_level`	Нет	Уровень детализации файлов трассировки Сервера администрирования. Трассировка записывается во время работы Сервера администрирования. Значение по умолчанию – 0, трассировка не записывается. Возможные значения параметра: 0–5. Чем выше значение параметра, тем более подробная информация о трассировке записывается.
`ansible_extra_flags`	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • `-v` • `-vv` • `-vvv` • `-vvvv` По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.
`incident_attachments_max_count_limit`	Нет	Количество файлов, которые вы можете прикрепить к инциденту. По умолчанию указано значение `100`.
`incident_attachments_max_size_limit`	Нет	Общий размер файлов, прикрепленных к инциденту. Измеряется в байтах. Единицы измерения не отображаются. По умолчанию указано значение `26214400`.
`ignore_precheck`	Нет	Параметр, указывающий, следует ли проверить аппаратное и программное обеспечение, а также конфигурацию сети узлов кластера Kubernetes на соответствие требованиям, необходимым для установки решения перед развертыванием. Возможные значения параметра: • `true` – пропустить предварительные проверки. • `false` – выполнить предварительные проверки (значение по умолчанию).
`airgap_mode`	Нет	Параметр, включающий или выключающий предварительную проверку и обновление кеша пакетов пакетным менеджером APT. Таким образом становится возможным развертывание Kaspersky EDR Expert в среде с физической изоляцией. Возможные значения параметра: • `true` – пропустить предварительную проверку и обновление кеша пакетов. • `false` – выполнить предварительную проверку и обновление кеша пакетов (значение по умолчанию).
`grafana_smtp_host`	Нет	Адрес SMTP-сервера для Grafana, который используется для отправки уведомлений о событиях, связанных с работоспособностью кластера Kubernetes, по электронной почте. Укажите этот параметр в формате `<хост>:<порт>` – например, `localhost:25`.
`grafana_smtp_user`	Нет	Имя пользователя для аутентификации на SMTP-сервере.
`grafana_smtp_password`	Нет	Пароль для аутентификации на SMTP-сервере.
`grafana_smtp_bundle`	Нет	Файл, содержащий цепочку сертификатов X.509, которая используется для проверки TLS-подключения к SMTP-серверу.
`grafana_smtp_skip_verify`	Нет	Данный параметр указывает, следует ли пропускать проверку TLS-сертификата для SMTP-сервера. Возможные значения параметра: • `true` – пропустить проверку TLS-сертификата. • `false` – выполнять проверку TLS-сертификата (значение по умолчанию).
`grafana_smtp_from_address`	Нет	Электронный адрес отправителя, который будет отображаться в поле "От" при отправке уведомлений по электронной почте.
`grafana_smtp_from_name`	Нет	Отображаемое имя отправителя в уведомлениях по электронной почте.

Имя параметра	Обязательная	Описание
`grafana_smtp_ehlo_identity`	Нет	Идентификатор, используемый в команде EHLO при подключении к SMTP-серверу.
`grafana_starttls_policy`	Нет	Политика использования STARTTLS при подключении к SMTP-серверу. Возможные значения параметра: • `OpportunisticStartTLS` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования. • `MandatoryStartTLS` – требовать STARTTLS и завершаться с ошибкой, если SMTP-сервер не поддерживает STARTTLS. • `NoStartTLS` – не использовать STARTTLS и подключиться к SMPT-серверу без шифрования. • `empty` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования (значение по умолчанию).
`grafana_smtp_enable_tracing`	Нет	Параметр, который указывает, следует ли включить ли трассировку SMTP-подключения для отладки отправки электронной почты. Возможные значения параметра: • `true` – включить трассировку SMTP-подключения. • `false` – отключить трассировку SMTP-подключения (значение по умолчанию).
`autodeploy_plan`	Нет	Параметр, указывающий, следует ли развертывать сервисы KUMA для Kaspersky EDR или для Kaspersky NGFW. Возможные значения параметра: • `edr` – развернуть службы KUMA для OSMP и Kaspersky EDR в кластере Kubernetes (значение по умолчанию). • `ngfw` – развернуть службы KUMA для OSMP и Kaspersky NGFW внутри кластера Kubernetes. Также предустановленный коллектор **[OOTB] Kaspersky NGFW** будет установлен на первом устройстве из списка устройств, указанного в параметре `kuma_collector` файла инвентаря KUMA. • `none` – не разворачивать службы KUMA для Kaspersky EDR или Kaspersky NGFW. Это значение следует указывать при развертывании Kaspersky EDR Expert без сервисов KUMA для Kaspersky EDR и Kaspersky NGFW или при восстановлении Kaspersky EDR Expert из резервной копии. Если при восстановлении Kaspersky EDR Expert задать значения `edr` или `ngfw`, это может привести к конфликту между развернутыми сервисами и сервисами из резервной копии.
`feature_gost_status`	Нет	Параметр, который указывает использовать ли рабочий процесс, созданный на основании ГОСТ Р 59712-2022, для управления инцидентами. Значение по умолчанию `false`. Возможные значения параметра: • `true` – рабочий процесс по ГОСТ используется. • `false` – рабочий процесс по ГОСТ не используется.
`tokenhub_access_token`	Нет	Время жизни токена доступа. В конфигурационном файле установите значение параметра – "`<time in hours>h<time in minutes>m<time in seconds>s`". Например, "`1h10m`" или "`2h`". Минимальное значение – `5m`, а максимальное значение – `2h`. Значение по умолчанию – `1h`. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр `tokenhub_access_token` позже, после развертывания приложения.

Имя параметра	Обязательная	Описание
tokenhub_refresh_token	Нет	Время жизни токена обновления, используемого для получения нового токена доступа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1240h30m". Минимальное значение – 12m, а максимальное значение – 4320h. Значение по умолчанию – 24h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр tokenhub_refresh_token позже, после развертывания приложения.
credentials_session_ttl	Нет	Максимальное время простоя сеанса единого входа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1h30m". Минимальное значение – 5m, а максимальное значение – 96h. Значение по умолчанию – 1h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр credentials_session_ttl позже, после развертывания приложения.

Пример конфигурационного файла для развертывания Kaspersky EDR Expert на одном узле

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky EDR will be deployed
nodes:
  # Параметры управляющего рабочего узла.
    # Имя узла. Длина значения должна быть от 1 до 63 символов.
    # Имя узла может содержать только буквы ASCII (a–z; A–Z), цифры (0–9) и дефис (-).
  - desc: cdt-1
    # Тип узла.
    # Для развертывания на одном узле установите для параметра "type" значение "primary-
    worker". В этом случае целевое устройство будет действовать как управляющий и рабочий
    узлы.
    type: primary-worker
    # IP-адрес узла.
    # Управляющий рабочий узел должен быть включен в ту же подсеть, что и шлюз кластера
    Kubernetes.
    host: 10.80.23.42
    access:
      ssh:
        # Имя пользователя учетной записи.
        # Учетная запись пользователя создается на целевом устройстве и используется KDT
        для подключения к узлу.
        # Длина имени пользователя должна быть от 1 до 31 символов.
        # Имя пользователя может содержать буквы (a–z; A–Z), цифры (0–9) и дефис (-).
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
# Parameters for the Kaspersky EDR deployment
parameters:
```

```
# Строка подключения для доступа к СУБД, которая установлена и настроена на отдельном
сервере.
# user_db – имя пользователя привилегированной внутренней учетной записи СУБД. Этой
учетной записи предоставлены права на создание баз данных и других учетных записей
СУБД.
# password_db – пароль привилегированной внутренней учетной записи СУБД.
# fqdn_db:port_db – полное имя домена и порт подключения отдельного сервера, на котором
установлена СУБД.
# Значение параметра 'psql_dsn' должно соответствовать URI-формату. Если URI-
подключение включает специальные символы в любой из его частей, символы должны быть
экранированы с помощью процентной кодировки.
- name: psql_dsn
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# IP-адрес шлюза кластера Kubernetes.
# The Kubernetes cluster gateway is intended for connecting to the Kaspersky EDR
components installed inside the Kubernetes cluster.
# Шлюз кластера должен быть включен в ту же подсеть, что и управляющий рабочий узел
кластера.
- name: ingress_ip
  source:
    value: 10.80.23.182
# Путь к закрытой части SSH-ключа для подключения к управляющему рабочему узлу с
помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky EDR user account that will be created during the
installation.
# Длина пароля должна быть от 10 до 256 символов.
# Он может содержать строчные или прописные буквы (a–z; A–Z), цифры (0–9) и специальные
символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
# Пароль не должен содержать пробелы или сочетания символов ".@".
- name: admin_password
  source:
    value: ""
# The parameter indicating that Kaspersky EDR is installed on the target host with
limited computing resources.
# For the single-node deployment, set the 'low_resources' parameter to "true" so that
Kaspersky Symphony EDR components will require less memory and CPU resources.
# Если вы включите этот параметр, для установки Ядра KUMA на целевом устройстве будет
выделено 4 ГБ свободного дискового пространства.
- name: low_resources
  source:
    value: "true"
# The number of disk volumes that are used to store the service data of Kaspersky EDR
components and KDT.
# Для развертывания на одном узле установите для параметра значение "1".
- name: default_class_replica_count
  source:
    value: "1"
# Параметр, который указывает, следует ли запускать хранилище секретов в режиме High
Availability (HA).
# Для развертывания на одном узле установите для параметра значение "false".
- name: openbao_ha_mode
  source:
```

```
    value: "false"
# Параметр, который указывает, следует ли запускать хранилище секретов в автономном
режиме.
# Для развертывания на одном узле установите для параметра значение "true".
- name: openbao_standalone
  source:
    value: "true"
# Путь к файлу инвентаря KUMA, который содержит параметры установки для развертывания
сервисов KUMA. Этот файл расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Путь к лицензионному ключу Kaspersky Endpoint Detection and Response. Этот файл
расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: license
  source:
    value: "/home/user/license.key"
# Имя домена. Значение параметра должно соответствовать требованиям назначения имен
доменов второго уровня.
# The service host name and domain name are parts of FQDNs of the Kaspersky EDR
services.
# Значения по умолчанию для имен служб устройств: nwc_host—"console", flow_host
—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host
—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Пользовательские имена устройств могут быть указаны в конфигурационном файле.
# Пример: console.smp.local является FQDN службы, предоставляющей доступ к Консоли
OSMP. Этот FQDN состоит из значений параметров 'console_host' и 'smp_domain'.
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky EDR services for which a self-signed or custom
certificate must be generated.
# Значение параметра должно быть списком имен устройств, разделенных пробелами. Если
пользовательские имена устройств не указаны, используются имена устройств по умолчанию:
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина имени пользователя должна быть от 1 до 30 символов.
# Имя пользователя может содержать строчные буквы (от 'a' до 'z'), цифры (от '0' до
'9') и специальные символы (_ - .).
# Имя пользователя должно начинаться с буквы и не должно содержать пробелы или символ
"@".
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью
инструмента Grafana.
# Длина пароля должна быть от 8 до 256 символов.
```

```
# Он может содержать строчные или прописные буквы (a-z; A-Z), цифры (0-9) и специальные
символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

Подключение компонентов Endpoint Agent через прокси-узел

В этом разделе описан сценарий развертывания Endpoint Agents для Kaspersky EDR Expert и серверов, которым они передают данные, если находятся в разных сетях. Такой подход упрощает настройку сети, обеспечивая при этом надежное подключение между Endpoint Agents и серверами.

В этом сценарии данные от Endpoint Agent, передаются через промежуточный прокси-узел. Это позволяет установить одно сетевое соединение между прокси-узлом и решением, вместо того, чтобы устанавливать несколько соединений от каждого Endpoint Agent к решению. Этот подход может быть применен как к развертыванию Kaspersky EDR Expert на одном узле, так и к развертыванию на нескольких узлах.

В разделе описана настройка прокси-сервера Nginx на Linux-устройстве. Допускается использование другого прокси-сервера с поддержкой mTLS Passthrough и, если требуется, другой операционной системы.

В этом сценарии используются примеры FQDN публичных серверов Kaspersky EDR Expert, указанных при развертывании решения `<agentserver>.<smp_domain>`, `<ksc_host>.<smp_domain>` и `<kuma_host>.<smp_domain>`), а также пути к файлам и директориям. Вам нужно заменить эти значения соответствующими значениями для вашей инфраструктуры.

Если вы изменили порт, используемый Endpoint Agents для подключения к компоненту agentserver, вам также нужно указать новый номер порта в конфигурационном файле Nginx.

Этапы развертывания

Развертывание с настройкой проксирования данных из Endpoint Agent через промежуточный прокси-узел состоит из следующих этапов:

1. **Установка и настройка Nginx**

   Установите прокси-сервер Nginx на сервер, расположенный в той же сети (или подсети), где расположен Endpoint Agent.

   1. Выполните следующие команды:

      ```
      sudo apt update
      sudo apt install nginx-full
      ```

   2. Убедитесь, что модули `stream`, `stream_ssl` и `stream_ssl_preread` добавлены в Nginx и загружены:

      ```
      nginx -V 2>&1 | grep -E 'stream|stream_ssl|stream_ssl_preread
      ```

      В выводе команды должны быть упомянуты модули `stream`, `stream_ssl` и `stream_ssl_preread`.

      На сервере установлен прокси-сервер Nginx с модулями `stream`, `stream_ssl` и `stream_ssl_preread`.

3. Убедитесь, что конфигурационный файл Nginx (по умолчанию /etc/nginx/nginx.conf) содержит блок `stream {}`, и что в этом блоке настроено подключение к директории `stream.d`. Если блок `stream` отсутствует, добавьте этот блок на том же уровне, что и блок `http {}`:

```
/etc/nginx/nginx.conf
...
http {
    ...
}

stream {
    include /etc/nginx/stream.d/*.conf;
}
```

4. Создайте или отредактируйте в соответствии с приведенным ниже шаблоном файл конфигурации NGINX в формате CONF в директории /etc/nginx/stream.d/.

   Если директория /etc/nginx/stream.d/ не существует, создайте ее.

   Путь и имя конфигурационного файла Nginx: /etc/nginx/stream.d/asproxy.conf.

   Переменные шаблона (подставьте значения, соответствующие вашей инфраструктуре):

   FQDN хостов публичных сервисов Kaspersky EDR Expert, с которыми взаимодействует Endpoint Agent:

   - `<agentserver>.<smp_domain>` – FQDN компонента, позволяющего выполнять действия по реагированию над активами с помощью интеграции с агентом.
   - `in.<какие-либо_символы>.<kuma_host>.<smp_domain>` – FQDN целевого backend-сервера для телеметрии.

     Способы получения адреса сервера

     1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и службы** → **Работа с сервисами** → **Активные сервисы**.
     2. В списке служб найдите службу **[OOTB] Kaspersky EDR**, выберите его и в меню выберите **Развернуть**.
     3. В открывшемся окне скопируйте адрес сервера из поля **URL шлюза API**.

        Имя сервера должно соответствовать формату – `in.blh4zjhm4edckdt8qyprkpm2b.kuma_host.smp_domain`.
   - `<kuma_host>.<smp_domain>` – FQDN целевого backend-сервера для управления агентом. Это может быть FQDN компонента OSMP для управления Endpoint Agent или FQDN подчиненного Сервера администрирования Kaspersky Security Center.

   IP-адреса:

   - `<ingress_ip>` – IP-адрес на входе кластера OSMP.
   - `<ksc_ip>` – IP-адрес подчиненного Сервера OSMP или KSC (если таковой используется).

   Существует три способа подключения агентов Endpoint Agent:

   - С помощью политики. В этом случае настройте проксирование для обмена данными между Endpoint Agent и прокси-сервером Nginx: укажите `<ksc_host>.<smp_domain>` и порты TCP 13000, TCP 14000 и TCP 13292.

Пример

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;

map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}

# ----- Backends-------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ingress_ip>:13000;
    server <ingress_ip>:14000;
    server <ingress_ip>:13292;
}
upstream deny-backend {
    server 127.0.0.1:1;
}

# ----- Logging--------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;

# ----- Timeouts-------------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;

# ----- Server (port 443) ---------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- Через политику на подчиненном сервере OSMP или KSC. В этом случае настройте проксирование для обмена данными между Endpoint Agent и прокси-сервером Nginx: укажите `<ksc_host>.<smp_domain>` и порты TCP 13000, TCP 14000 и TCP 13292.

Пример

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;

map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}

# ----- Backends-------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ksc_ip>:13000;
    server <ksc_ip>:14000;
    server <ksc_ip>:13292;
}
```

```
upstream deny-backend {
    server 127.0.0.1:1;
}

# ----- Logging-------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;

# ----- Timeouts----------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;

# ----- Server (port 443) -------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- Локально. В этом случае на прокси-сервере Nginx не нужно настраивать `<ksc_host>.<smp_domain>` и TCP-порты. Подробнее см. шаг 3 этого сценария.

Пример

```
# ----- SNI → upstream ----------------------------------------------
map_hash_bucket_size 256;

map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    default                           deny-backend;
}

# ----- Backends------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}

upstream deny-backend {
    server 127.0.0.1:1;
}

# ----- Logging-------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;

# ----- Timeouts----------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;

# ----- Server (port 443) -------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

5. Проверьте конфигурацию NGINX:

```
nginx -t
```

Вывод команды при успешном прохождении теста:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

6. Перезагрузите NGINX для применения изменений в конфигурационном файле:

```
nginx -s reload
```

Установленный прокси-сервер Nginx настроен для проксирования данных Endpoint Agent.

2 Настройка связи по сети между прокси-узлом NGINX и Kaspersky EDR Expert

1. Настройка сетевых подключений. Убедитесь, что параметры сети (сетевой экран, маршрутизация) разрешают исходящие подключения от прокси-сервера к платформе OSMP и вторичному серверу OSMP или KSC через порты TCP 13000, TCP 14000, TCP 13292 и TCP 443.

2. Конфигурация сети должна обеспечивать маршутизацию запросов узлов Endpoint Agent к `<smp_domain>` на прокси-узел.

3 Настройка Endpoint Agent в Kaspersky Endpoint Security для Windows для работы через прокси-узел

1. Настройка сетевых подключений. Убедитесь, что параметры сети (сетевой экран, маршрутизация) разрешают исходящие подключения от Endpoint Agents к прокси-узлу через порты TCP 13000, TCP 14000, TCP 13292 и TCP 443.

2. Скачайте следующие сертификаты OSMP:

   - certificate.pem – сертификат сервера реагирования
   - certificate.pfx – сертификат Endpoint Agent
   - [OOTB] Kaspersky EDR – сертификат сервера телеметрии

3. Скопируйте файлы сертификатов на сервер, где установлен Endpoint Agent (для примера в этом разделе – C:\Users\TestUser\).

4. Откройте командную строку `cmd.exe` с правами администратора.

5. Перейдите в директорию, содержащую исполняемый файл Endpoint Agent, и выполните следующую команду:

```
./avp.com EDREXPERTONPREM `
/SET /mode=EDRExpertOnPrem `
/servers=<agentserver>.<smp_domain>:443 `
/server-certificate=C:\Users\TestUser\certificate.pem `
/client-certificate=C:\Users\TestUser\certificate.pfx `
/client-certificate-password=client certificate password`
/telemetry-servers=in.blh4zjhm4edckdt8qyprkpm2b.<kuma_host>.<smp_domain>:443 `
/telemetry-server-certificate='C:\Users\TestUser\[OOTB] Kaspersky EDR' `
/telemetry-client-certificate=C:\Users\TestUser\certificate.pfx `
/telemetry-client-certificate-password=client certificate password
```

6. Запустите Kaspersky EDR Expert, если решение еще не запущено:

```
./avp.com start EDREXPERTONPREM
```

Подробнее о настройке Endpoint Agent с помощью командной строки см. в документации Kaspersky Endpoint Security.

Мастер развертывания для Kaspersky EDR Expert

Подготовка среды для развертывания Kaspersky EDR Expert включает несколько шагов, которые необходимо выполнить вручную, такие как настройка параметров установки, подготовка целевых устройств и проверка системных требований. Мастер развертывания позволяет указать параметры установки, необходимые для развертывания Kaspersky EDR Expert, а затем сформировать конфигурационный файл. Дополнительные параметры установки используют значения по умолчанию и недоступны в мастере развертывания. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения по умолчанию.

Мастер развертывания автоматически проверяет готовность целевых устройств к развертыванию, включая подключение по SSH, доступность нужных портов, уникальность IP-адреса, разрешение DNS-имен на узлах кластера и синхронизацию времени. При обнаружении проблем мастер отображает сообщение об ошибке с описанием проблемы. После успешного завершения всех проверок вы можете сохранить сгенерированный конфигурационный файл или продолжить развертывание Kaspersky EDR Expert.

> В настоящее время мастер развертывания поддерживает только развертывание на одном узле.

Предварительные требования

- Установить систему управления базами данных.

  Перед развертыванием Kaspersky EDR Expert в конфигурации на одном узле необходимо вручную установить СУБД на целевое устройство. СУБД и компоненты Kaspersky EDR Expert устанавливаются на одном и том же устройстве, но СУБД будет развернута вне кластера Kubernetes.

- Выполните все подготовительные шаги, необходимые для устройства администратора, целевых устройств и устройств KUMA (если сервисы KUMA будут установлены на отдельных серверах вне кластера).

Процесс

Чтобы указать параметры установки с помощью мастера развертывания:

1. На устройстве администратора, на котором расположена утилита KDT, запустите мастер развертывания с помощью следующей команды:

   ```
   ./kdt wizard -k <путь_к_транспортному_архиву> -o <путь_к_конфигурационному_файлу>
   ```

   где:

   - `<path_to_transport_archive>` – путь к транспортному архиву. Это необязательный параметр, вы можете указать его позже.
   - `<path_to_configuration_file>` – путь, по которому вы хотите сохранить конфигурационный файл и имя конфигурационного файла. Это необязательный параметр, вы можете указать его позже.

   Мастер развертывания предложит вам указать параметры установки.

   Если у вас нет прав на запись в указанной директории или в этой директории находится файл с таким же именем, возникает ошибка и мастер завершает работу.

2. Введите путь к транспортному архиву.

   Если вы указали этот параметр при запуске мастера развертывания, он заполняется автоматически.

3. Введите путь к конфигурационному файлу.

   Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если вы указали этот параметр при запуске мастера развертывания, он заполняется автоматически.

4. Введите IPv4-адрес управляющего рабочего узла (параметр `host` в конфигурационном файле).

   Этот узел должен быть включен в ту же подсеть, что и IP-адрес шлюза кластера.

5. Введите имя пользователя учетной записи, используемой для подключения к управляющему рабочему узлу с помощью KDT (параметр `user` конфигурационного файла).

   Значение должно соответствовать следующим правилам:

   - Длина имени пользователя должна быть от 1 до 31 символов.
   - Имя пользователя может содержать следующие символы:
     - нижний регистр (a-z);
     - числа (0–9);
     - нижнее подчеркивание (_), дефис (-).

6. Введите пароль для подключения к узлу (параметр `password` в конфигурационном файле).

   Пароль можно использовать вместо SSH-ключа.

7. Введите строку подключения для доступа к СУБД (параметр `psql_dsn` в конфигурационном файле).

Укажите этот параметр следующим образом: `postgres://<dbms_username>:<password>@<fqdn>:<port>`

где:

- `dbms_username` – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Kaspersky EDR Expert.
- `password` – пароль привилегированной внутренней учетной записи СУБД.
- `fqdn:port` – полное имя домена и порт подключения целевого устройства, на котором установлена СУБД.

  Для развертывания на одном узле, если ваша СУБД установлена на том же узле, что и узел кластера Kubernetes, не используйте `localhost` или `127.0.0.1` в качестве адреса сервера СУБД в строке подключения. Вместо этого используйте FQDN или IP-адрес устройства.

> Мастер развертывания задает параметры установки только для варианта развертывания с установленной СУБД вне кластера Kubernetes.

8. Введите путь к файлу инвентаря KUMA, расположенному на устройстве администратора (параметр `inventory` конфигурационного файла).

   Файл инвентаря KUMA содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.

   Если сервисы KUMA устанавливаются в кластере Kubernetes, укажите путь `/dev/null`.

9. Выберите язык интерфейса Консоли OSMP. После установки вы можете изменить язык Консоли OSMP (параметр `nwc-language` в конфигурационном файле).

   Возможные значения:

   - enUS
   - ruRu

10. Введите пароль учетной записи Kaspersky EDR Expert, которая будет создана KDT при установке (параметр `admin_password` конфигурационного файла).

    Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора.

    Пароль должен соответствовать следующим правилам:

    - Пароль пользователя не может содержать менее 10 или более 256 символов.
    - Пароль должен содержать символы как минимум трех указанных ниже групп:
      - верхний регистр (A–Z);
      - нижний регистр (a-z);

    - числа (0–9);
    - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Пароль не должен содержать пробелов или комбинации ".@".

11. Введите IPv4-адрес шлюза кластера Kubernetes (параметр `ingress_ip` конфигурационного файла).

    Шлюз кластера должен быть включен в ту же подсеть, что и управляющий рабочий узел кластера.

12. Введите имя пользователя учетной записи, используемой для просмотра метрик OSMP с помощью утилиты Grafana (параметр `grafana_admin_user` в конфигурационном файле).

    Значение должно соответствовать следующим правилам:

    - Длина имени пользователя должна быть от 1 до 30 символов.
    - Имя пользователя может содержать следующие символы:
      - нижний регистр (a-z);
      - числа (0–9);
      - специальные символы (_ - .)
    - Имя пользователя должно начинаться с буквы.
    - Имя пользователя не должно содержать пробелов или символа "@".

13. Введите пароль учетной записи, используемой для просмотра метрик OSMP с помощью утилиты Grafana (параметр `grafana_admin_password` в конфигурационном файле).

    Пароль должен соответствовать следующим правилам:

    - Пароль пользователя не может содержать менее 8 или более 256 символов.
    - Пароль должен содержать символы из указанных ниже групп:
      - верхний регистр (A–Z);
      - нижний регистр (a-z);
      - числа (0–9);
      - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

14. Чтобы указать параметр `extended_incident_lifecycle`, пропустите этот шаг. Это служебный параметр. По умолчанию параметр `extended_incident_lifecycle` отключен, не изменяйте его.

15. Введите имя домена, которое используется в FQDN публичных сервисов Kaspersky EDR Expert (параметр `smp_domain` конфигурационного файла).

    Значение параметра должно соответствовать требованиям назначения имен доменов второго уровня.

16. Введите имена устройств, которые используются в FQDN публичных сервисов Kaspersky EDR Expert (параметры `nwc_host`, `flow_host`, `hydra_host`, `login_host`, `ksc_host`, `console_host`, `api_host`, `kuma_host`, `monitoring_host`, `xdr_edr_ingress_host` конфигурационного файла).

Если пользовательские имена устройств не указаны, используются следующие имена устройств по умолчанию:

- `nwc_host - "console"`
- `flow_host - "console"`
- `hydra_host - "console"`
- `login_host - "console"`
- `ksc_host—"admsrv"`
- `console_host - "console"`
- `api_host - "api"`
- `kuma_host - "kuma"`
- `monitoring_host - "monitoring"`
- `xdr_edr_ingress_host—"agentserver"`

Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.

17. Выберите `Проверить`, чтобы проверить сгенерированный конфигурационный файл, или `Пропустить`, чтобы продолжить без проверки.

18. Выберите `Сохранить и выйти`, чтобы сохранить сгенерированный конфигурационный файл в формате YAML с указанными параметрами. Остальные параметры установки включены в конфигурационный файл со значениями по умолчанию. Вы можете изменить конфигурационный файл вручную перед развертыванием Kaspersky EDR Expert. Выберите `Установить`, чтобы начать развертывание Kaspersky EDR Expert с этим конфигурационным файлом.

Мастер развертывания сохраняет конфигурационный файл с указанными параметрами в формате YAML и запускает развертывание Kaspersky EDR Expert.

Установка Kaspersky EDR Expert

Kaspersky EDR Expert разворачивается с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Kaspersky EDR Expert и другие компоненты инфраструктуры. Шаги установки Kaspersky EDR Expert не зависят от выбранного варианта развертывания.

Если вам нужно установить несколько кластеров Kubernetes с экземплярами Kaspersky EDR Expert, вы можете использовать необходимое количество контекстов.

Чтобы установить Kaspersky EDR Expert:

1. Распакуйте загруженный дистрибутив с KDT на устройство администратора.

2. Ознакомьтесь с Лицензионным соглашением KDT, находящимся в дистрибутиве с компонентами Kaspersky EDR Expert.

   Когда вы начинаете использовать KDT, вы принимаете условия Лицензионного соглашения KDT.

   Вы можете ознакомиться с Лицензионным соглашением KDT после установки Kaspersky EDR Expert. Файл `license_kdt.txt` находится в директории `~/kaspersky_eula` пользователя, который запускает развертывание Kaspersky EDR Expert.

3. Во время установки KDT загружает недостающие пакеты из хранилищ операционной системы. Перед установкой Kaspersky EDR Expert, выполните следующую команду на целевых устройствах, чтобы убедиться, что кеш apt/yum актуален.

   ```
   apt update
   ```

4. Перезагрузите целевые устройства.

5. На устройстве администратора выполните следующие команды, чтобы начать развертывание Kaspersky EDR Expert с помощью KDT. Укажите путь к транспортному архиву с компонентами Kaspersky EDR Expert и путь к конфигурационному файлу, который вы заполнили ранее (наборы параметров установки для развертывания на нескольких узлах и развертывания на одном узле различаются).

   ```
   chmod +x kdt
   ./kdt apply -k <полный_путь_к_транспортному_архиву> -i
   <полный_путь_к_конфигурационному_файлу>
   ```

   Вы можете установить Kaspersky EDR Expert без запроса на ознакомление с условиями Лицензионного соглашения и Политикой конфиденциальности OSMP, если вы используете флаг `--accept-eula`. В этом случае вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности OSMP перед установкой Kaspersky EDR Expert. Файлы находятся в дистрибутиве с компонентами Kaspersky EDR Expert.

   Если вы хотите прочитать и принять условия Лицензионного соглашения и Политики конфиденциальности во время развертывания, не используйте флаг `--accept-eula`.

   Если при развертывании Kaspersky EDR Expert с помощью KDT возникла ошибка, запустите развертывание заново, указав путь к конфигурационному файлу без флага `-i`.

6. Если вы не использовали флаг `--accept-eula` на предыдущем шаге, прочтите Лицензионное соглашение и Политику конфиденциальности OSMP. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

      Введите `n`, если вы не принимаете условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны) в соответствии с Политикой конфиденциальности.

      Введите `n`, если вы не принимаете условия Политики конфиденциальности.

      > Чтобы использовать Kaspersky EDR Expert, вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности.

После того как вы начнете развертывание, KDT проверяет, соответствуют ли аппаратное и программное обеспечение, а также сетевая конфигурация узлов кластера Kubernetes необходимым условиям для установки решения. Если все строгие предварительные проверки успешно пройдены, KDT разворачивает компоненты Kaspersky EDR Expert в кластере Kubernetes на целевых устройствах. В ином случае развертывание будет прервано. Вы можете пропустить предварительные проверки перед развертыванием, если это необходимо (укажите для параметра установки `ignore_precheck` значение `true`).

Также утилита KDT проверяет, правильно ли указаны необходимые параметры установки. Если необходимые параметры в конфигурационном файле отсутствуют или недействительны, развертывание будет прервано. Правила, которых следует придерживаться при установке значений параметров, указаны в шаблонах конфигурационных файлов (multinode.smp_param.yaml.template и singlenode.smp_param.yaml.template).

> При развертывании Kaspersky EDR Expert на главном Сервере администрирования создается пользователь. Чтобы начать настройку Консоли OSMP, этому пользователю назначаются следующие роли: EDR-роль Главного администратора в корневом тенанте и роль Главного администратора в Kaspersky Security Center.

7. Просмотрите журналы событий установки компонента Bootstrap в директории с утилитой KDT и при необходимости получите диагностическую информацию о компонентах Kaspersky EDR Expert.

8. Войдите в Консоль OSMP.

   Адрес Консоли OSMP по умолчанию – `https://<console_host>.<smp_domain>:443`.

   Адреса состоят из значений параметров `console_host` и `smp_domain`, указанных в конфигурационном файле.

Kaspersky EDR Expert развернут на целевых устройствах. Установите сервисы KUMA, чтобы начать работу с решением.

Настройка доступа в интернет целевых устройств

Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, а также нужно подключить целевые устройства к интернету, вам необходимо добавить IP-адрес каждого целевого устройства в переменную `no_proxy` в файле /etc/environment перед развертыванием Kaspersky EDR Expert. Это позволяет установить прямое подключение целевых устройств к интернету и правильно развернуть Kaspersky EDR Expert.

Чтобы настроить доступ целевых устройств в интернет:

1. На целевом устройстве откройте файл /etc/environment с помощью текстового редактора. Например, следующая команда открывает файл с помощью текстового редактора GNU nano:

   ```
   sudo nano /etc/environment
   ```

2. В файл /etc/environment добавьте IP-адрес целевого устройства в переменную `no_proxy` через запятую без пробела.

   Например, переменную `no_proxy` можно изначально указать следующим образом:

   ```
   no_proxy=localhost,127.0.0.1
   ```

   Вы можете добавить IP-адрес целевого устройства (192.168.0.1) в переменную `no_proxy`:

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.1
   ```

   Также вы можете указать подсеть, в которую входят целевые устройства (в нотации CIDR):

```
no_proxy=localhost,127.0.0.1,192.168.0.0/24
```

3. Сохраните файл /etc/environment.

4. Перезагрузите целевое устройство:

```
reboot
```

После добавления IP-адресов в файл /etc/environment к каждому целевому устройству и перезагрузки целевых устройств можно продолжить их подготовку и дальнейшее развертывание Kaspersky EDR Expert.

Синхронизация времени на машинах

Чтобы настроить синхронизацию времени на машинах:

1. Выполните команду, чтобы установить chrony:

```
sudo apt install chrony
```

2. Настройте системное время для синхронизации с NTP-сервером:

   a. Убедитесь, что у виртуальной машины есть доступ в интернет.

   Если доступ есть, переходите к шагу b.

   Если доступ в интернет отсутствует, замените текущие общедоступные источники (начиная с `пула`) в файле `/etc/chrony.conf` именем или IP-адресом внутреннего NTP-сервера вашей организации.

   b. Запустите службу синхронизации системного времени, выполнив следующую команду:

```
sudo systemctl enable --now chrony
```

   c. Подождите несколько секунд и выполните команду:

```
sudo timedatectl | grep 'System clock synchronized'
```

   Если системное время синхронизировано правильно, в выводе будет строка `System clock synchronized: yes`.

Синхронизация настроена.

Установка сервисов KUMA внутри кластера Kubernetes

Службы – это основные компоненты SIEM-системы KUMA, которые помогают системе управлять событиями. Сервисы позволяют получать события из источников событий и в дальнейшем приводить их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа.

Типы сервисов:

- Хранилища используются для хранения событий.
- Коллекторы используются для получения событий и преобразования их в формат KUMA.

> Если вы планируете использовать несколько тенантов в своей инфраструктуре, создайте отдельный коллектор для каждого тенанта.

- Корреляторы используются для анализа событий и поиска закономерностей.
- Агенты используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

Устанавливать сервисы KUMA можно только после развертывания Kaspersky EDR Expert. При развертывании Kaspersky EDR Expert подготавливается необходимая инфраструктура: на подготовленных устройствах создаются служебные директории, в которые добавляются файлы, необходимые для установки сервиса. Рекомендуется устанавливать сервисы в следующем порядке: хранилище, коллекторы, корреляторы и агенты.

Ограничения

При установке сервисов KUMA внутри кластера Kubernetes, учитывайте следующие ограничения:

- При установке можно развернуть только один экземпляр Ядра KUMA.
- Пассивные коллекторы могут быть развернуты, только если используются коннекторы HTTP или TCP с включенным TLS.
- Для пассивных коннекторов HTTP и TCP настроенные адрес сервера и порт автоматически заменяются на `0.0.0.0:7310`.
- Кластер хранилища должен быть развернут либо полностью внутри Kubernetes либо полностью вне кластера. Смешанные развертывания не поддерживаются.
- Если коллекторы или корреляторы, развернутые вне Kubernetes, отправляют события службам хранилища, развернутым внутри Kubernetes, доставка событий выполняется через один входящий URL. Балансировка нагрузки между узлами хранилища выполняется Kubernetes на уровне TCP.
- Если трафик должен быть направлен в разные группы узлов хранилища, вам нужно развернуть отдельные сервисы eventRouter и направить трафик через них.
- При изменении параметров коллектора, развернутого внутри кластера Kubernetes, KUMA не проверяет измененные параметры. Из-за неправильной настройки коллектор может не получать события.
- В одном кластере Kubernetes невозможно развернуть несколько сервисов хранения, созданных на основе одного и того же ресурса хранения, используя одно и то же значение **FQDN узла хранилища**.

Чтобы установить и настроить сервисы KUMA внутри кластера Kubernetes:

1. Убедитесь, что устройство администратора и целевые устройства для Kaspersky EDR Expert подготовлены в соответствии с выбранной схемой развертывания, выполнив одну из следующих инструкций:
   - Развертывание на нескольких узлах: подготовка устройства администратора и целевых устройств
   - Развертывание на одном узле: подготовка устройства администратора и целевых устройств
2. В Консоли OSMP создайте набор ресурсов для каждого сервиса KUMA (хранилища, коллекторы и корреляторы).
3. Создайте сервисы для хранилищ, коллекторов и корреляторов.

4. **Разверните каждую службу в кластере Kubernetes**.

   1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и службы** → **Активные службы**.

   2. Выберите службы, которую вы хотите развернуть, и нажмите на кнопку **Развернуть**.

   3. В окне **Добавить службу в Kubernetes** заполните следующие поля:

      - **FQDN узла хранилища**: укажите имя узла кластера хранилища, определенного в ресурсе хранилища. Этот параметр доступен только для службы хранилища и не может быть изменен после развертывания службы.

      - **Класс хранения**: выберите подсистему хранения, используемую для хранения статуса службы. Значение этого параметра невозможно изменить после развертывания. Доступные значения:

        - **longhorn** – этот класс хранилищ обеспечивает сетевое хранилище с поддержкой репликации. По умолчанию статус службы реплицируется на трех сетевых дисках. Этот класс хранилища рекомендуется для коллекторов, коррелятора, метрик и служб Ядра, поскольку он позволяет Kubernetes перенести под службы на другой рабочий узел в случае сбоя текущего узла. Его также можно использовать для обеспечения отказоустойчивости службы хранилища, развернутого как единый экземпляр.

        - **local-path** – этот класс хранилища использует локальные дисковые массивы рабочих узлов Kubernetes, монтированных в директории /opt/lvp/hot, и обеспечивает максимальную производительность. Этот класс хранилища рекомендуется использовать для службы хранилища, поскольку хранилище поддерживает собственную кластеризацию и не использует механизмы Kubernetes для обеспечения отказоустойчивости. Его также можно использовать для служб коллектора, использующих коннекторы HTTP или TCP, и для служб eventRouter, развернутых на нескольких экземплярах, созданных из одного ресурса KUMA. При развертывании на одном узле рекомендуется использовать **local-path** для всех типов служб KUMA.

      - **Класс холодного хранения**: выберите подсистему хранилища, используемую для длительного хранения данных. Этот параметр доступен только для служб хранилища и не может быть изменен после развертывания. Класс хранилища **local-path-cold** похож на **local-path**, но предназначен для длительного хранения на более медленных дисковых массивах, монтированных в директории /opt/lvp/cold.

      - **Минимальное количество CPU**: укажите количество ядер процессора (потоков), зарезервированных для службы. Допускается указать целое положительное число. По умолчанию указано значение `0`.

      - **Максимальное количество CPU**: укажите максимальное количество ядер процессора (потоков), доступных для службы. Значение должно быть положительным целым числом и не может быть меньше значения в поле **Минимальное количество CPU**. По умолчанию указано значение `0`.

      - **Минимальный объем ОЗУ**: укажите объем оперативной памяти в ГБ, зарезервированной для службы. Допускается указать целое положительное число. По умолчанию указано значение `0`.

      - **Максимальный объем ОЗУ**: укажите максимальный объем оперативной памяти в ГБ, доступный для службы. Значение должно быть положительным целым числом и не может быть меньше значения в поле **Минимальный объем ОЗУ**. По умолчанию указано значение `0`.

- **Дисковое пространство, ГБ**: укажите объем дискового пространства в ГБ, выделенного для службы. Этот параметр доступен только при использовании класса хранилища **longhorn**.

- **Дисковое пространство холодного хранилища, ГБ**: укажите объем дискового пространства в ГБ, выделенного для длительного хранения данных. Этот параметр доступен только для службы хранилища, использующих класс хранилища **longhorn**.

4. Нажмите на кнопку **Создать службу**.

5. При необходимости убедитесь, что коллектор и коррелятор готовы к получению событий.

6. При необходимости установите агенты в сетевую инфраструктуру KUMA.

   Файлы, необходимые для установки агента, находятся в директории `/opt/kaspersky/kuma/utils`.

Необходимые для работы Kaspersky EDR Expert сервисы KUMA установлены внутри кластера Kubernetes.

Установка сервисов KUMA вне кластера Kubernetes

Сервисы – это основные компоненты KUMA, которые помогают системе управлять событиями. Сервисы позволяют получать события из источников событий и в дальнейшем приводить их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа.

Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены полностью внутри кластера на рабочих узлах, полностью на отдельных узлах вне кластера Kubernetes или частично внутри и частично вне кластера Kubernetes.

Типы сервисов:

- Хранилища используются для хранения событий.

- Коллекторы используются для получения событий и преобразования их в формат KUMA.

  > Если вы планируете использовать несколько тенантов в своей инфраструктуре, создайте отдельный коллектор для каждого тенанта.

- Корреляторы используются для анализа событий и поиска закономерностей.

- Агенты используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

Устанавливать сервисы KUMA можно только после развертывания Kaspersky EDR Expert. При развертывании Kaspersky EDR Expert подготавливается необходимая инфраструктура: на подготовленных устройствах создаются служебные директории, в которые добавляются файлы, необходимые для установки сервиса. Рекомендуется устанавливать сервисы в следующем порядке: хранилище, коллекторы, корреляторы и агенты.

Чтобы установить и настроить сервисы KUMA вне кластера Kubernetes:

1. В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.

2. В разделе KUMA Консоли OSMP создайте набор ресурсов для каждого сервиса KUMA (хранилищ, коллекторов и корреляторов), который вы хотите установить на подготовленных устройствах в сетевой инфраструктуре.

3. Создайте сервисы для хранилищ, коллекторов и корреляторов.

4. Получите идентификаторы сервисов для привязки созданных наборов ресурсов и сервисов KUMA:

   a. В решении OSMP перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. На подготовленных устройствах в сетевой инфраструктуре выполните соответствующие команды для установки сервисов KUMA. Используйте идентификаторы сервисов, которые были получены ранее:

   - Команда установки хранилища:

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the
     KUMA Core CA certificate> --id <service ID> --install
     ```

   - Команда установки коллектора:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port>
     ```

   - Команда установки коррелятора:

     ```
     sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
     ```

     где:

     - <FQDN> – полное доменное имя сервера Ядра KUMA.

     - <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

       Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

       Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

       Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

     - <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.

     - <API port> – это порт, используемый для связи с установленным компонентом.

   По умолчанию полное доменное имя Ядра KUMA – `<kuma_host>.<smp_domain>`.

   Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

Откройте порты, соответствующие установленному коллектору и коррелятору на сервере (TCP 7221 и другие порты, используемые для установки сервисов в качестве значения параметра `--api.port <port>`).

6. Во время установки сервисов KUMA прочтите Лицензионное соглашение KUMA. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.
   - Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать сервисы KUMA, вам нужно принять условия Лицензионного соглашения.

   Вы можете прочитать Лицензионное соглашение KUMA после установки сервисов KUMA одним из следующих способов:

   - На устройствах, входящих в группу `kuma_utils` в файле инвентаря KUMA, откройте файл LICENSE, расположенный в директории `/opt/kaspersky/kuma/utils`.
   - На устройствах, входящих в другие группы (`kuma_storage, kuma_collector` или `kuma_correlator`) в файле инвентаря KUMA, откройте файл LICENSE, расположенный в директории `/opt/kaspersky/kuma`.
   - Выполните следующую команду:

     ```
     /opt/kaspersky/kuma/kuma license --show
     ```

   После того как вы примете Лицензионное соглашение, сервисы KUMA будут установлены на подготовленных машинах в сетевой инфраструктуре.

7. При необходимости убедитесь, что коллектор и коррелятор готовы к получению событий.

8. При необходимости установите агенты в сетевую инфраструктуру KUMA.

   Файлы, необходимые для установки агента, находятся в директории `/opt/kaspersky/kuma/utils`.

Необходимые для работы Kaspersky EDR Expert сервисы KUMA установлены.

Развертывание нескольких кластеров Kubernetes и экземпляров Kaspersky EDR Expert

KDT позволяет развернуть несколько кластеров Kubernetes с экземплярами Kaspersky EDR Expert и переключаться между ними с помощью контекстов. *Контекст* – это набор параметров доступа, определяющих кластер Kubernetes, с которым пользователь может выбрать взаимодействие. Контекст также включает данные для подключения к кластеру с помощью KDT.

Предварительные требования

Перед созданием контекстов и установкой кластеров Kubernetes с экземплярами Kaspersky EDR Expert необходимо выполнить следующие действия:

1. Подготовить устройство администратора и целевые устройства.

   Для установки нескольких кластеров и экземпляров Kaspersky EDR Expert вам нужно подготовить одно устройство администрирования для всех кластеров и отдельные наборы целевых устройств для каждого кластера. Компоненты Kubernetes не следует устанавливать на целевые устройства.

2. Подготовить устройства к установке сервисов KUMA.

   Для установки сервисов KUMA вам нужно подготовить отдельные наборы устройств для каждого экземпляра Kaspersky EDR Expert.

3. Подготовить файл инвентаря KUMA.

   Для установки сервисов KUMA вам нужно подготовить отдельные файлы инвентаря для каждого экземпляра Kaspersky EDR Expert.

4. Подготовить конфигурационный файл.

   Для установки нескольких кластеров и экземпляров Kaspersky EDR Expert вам нужно подготовить конфигурационные файлы для каждого экземпляра Kaspersky EDR Expert. В этих конфигурационных файлах укажите соответствующие устройства администратора и целевые устройства, а также другие параметры, специфичные для конкретного кластера и экземпляра Kaspersky EDR Expert.

Процесс

Чтобы создать контекст с кластером Kubernetes и экземпляром Kaspersky EDR Expert:

1. На устройстве администратора, на котором расположена утилита KDT, выполните команду и укажите имя контекста:

   ```
   ./kdt ctx --create <имя_контекста>
   ```

   Контекст с указанным именем создан.

2. Установите кластер Kubernetes и Kaspersky EDR Expert.

Кластер с экземпляром Kaspersky EDR Expert развернут в контексте. Создание контекста завершено. Когда вы получаете файлы журналов компонентов Kaspersky EDR Expert, файлы журналов содержат имя вашего текущего контекста.

Вы можете повторить эту процедуру, чтобы создать необходимое количество контекстов с установленными кластерами и экземплярами Kaspersky EDR Expert.

> Вам нужно развернуть кластер Kubernetes и экземпляр Kaspersky EDR Expert после создания контекста, чтобы завершить создание контекста. Если вы не выполните развертывание в контексте, а затем создадите другой контекст, первый контекст будет удален.

Чтобы просмотреть список созданных контекстов и имя активного контекста,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt ctx
```

Чтобы переключиться на нужный контекст,

На устройстве администратора, на котором расположена утилита KDT, выполните команду и укажите имя контекста:

```
./kdt ctx <имя_контекста>
```

После выбора контекста KDT подключается к соответствующему кластеру Kubernetes. Теперь вы можете работать с этим кластером и экземпляром Kaspersky EDR Expert. К выбранному кластеру применяются команды KDT.

При удалении компонентов Kaspersky EDR Expert, установленных в кластере Kubernetes, и самого кластера с помощью KDT соответствующие контексты также удаляются. Другие контексты и их кластеры с экземплярами Kaspersky EDR Expert не удаляются.

Установка и обновление Kaspersky EDR Expert в среде с физической изоляцией

Kaspersky EDR Expert можно установить или обновить в среде с физической изоляцией. Установка и обновление в изолированной среде выполняются с помощью утилиты kdt-airgap-prepare и включают в себя следующие этапы:

1. Подготовка устройства администратора и целевых хостов, а также конфигурационного файла.
2. Получение информации о пакетах, установленных на целевых устройствах, находящихся в среде с физической изоляцией.

   Эта информация сравнивается со списком необходимых пакетов, после чего сведения о пакетах, отсутствующих на целевых устройствах, сохраняются в файле инвентаря YAML.
3. Загрузка необходимых пакетов, указанных в файле инвентаря, и зависящих от них пакетов из общедоступных хранилищ в Интернете или корпоративных зеркальных хранилищ в открытой среде.

   Загруженные пакеты сохраняются в локальном архиве пакетов TAR.
4. Установка или обновление пакетов и их зависимостей на целевых устройствах в изолированной среде из локального TAR-архива.
5. Установка или обновление Kaspersky EDR Expert в среде с физической изоляцией.

Подготовка устройства администратора и целевых устройств

Вам потребуется определить количество целевых устройств, на которых будет развертываться кластер Kubernetes и компоненты Kaspersky EDR Expert, входящие в этот кластер, с учетом выбранной схемы развертывания. Подготовьте устройство администратора и целевые устройства к развертыванию Kaspersky EDR Expert, выполнив одну из следующих инструкций (за исключением шагов, включающих загрузку и установку пакетов):

- Развертывание на нескольких узлах: подготовка устройства администратора и целевых устройств
- Развертывание на одном узле: подготовка устройства администратора и целевых устройств

Подготовьте конфигурационный файл в формате YAML. Конфигурационный файл содержит список целевых устройств для развертывания и набор параметров для установки компонентов Kaspersky EDR Expert.

Используйте конфигурационный файл, содержащий параметры установки, указанные для выбранной схемы развертывания:

- Развертывание на нескольких узлах: параметры установки
- Развертывание на одном узле: параметры установки

> При развертывании Kaspersky EDR Expert в среде с физической изоляцией, установите для параметра установки `airgap_mode` значение `true`.

Получение информации о пакетах, установленных на целевых устройствах, находящихся в среде с физической изоляцией.

Чтобы получить информацию об операционной системе и пакетах, установленных на целевых устройствах:

1. На устройстве администратора выполните команду. Укажите путь к закрытой части SSH-ключа, который находится на устройстве администратора и используется для подключения к целевым устройствам, путь к файлу конфигурации, который вы заполнили ранее, и путь к файлу инвентаря, в который будет сохранена информация:

   ```
   kdt-airgap-preparation scan -k <full_path_to_ssh_key> -c
   <full_path_to_configuration_file> --airgap -i <full_path_to_inventory_file>
   ```

   Утилите kdt-airgap-preparation сравнивает эту информацию со списком необходимых пакетов, после чего сведения о пакетах, отсутствующих на целевых устройствах, сохраняются в файле инвентаря YAML. Файл инвентаря YAML сохраняется в указанной директории с указанным именем.

Если вам нужно проверить наличие на целевых устройствах дополнительных пакетов, таких как Docker, выполните следующую команду:

```
kdt-airgap-preparation scan -k <full_path_to_ssh_key> -c
<full_path_to_configuration_file> --airgap -i <full_path_to_inventory_file> --add-pkgs
<package_name>
```

Информация о дополнительных пакетах, которые не установлены на целевых устройствах, добавляется в файл инвентаря YAML.

Созданный файл инвентаря будет использоваться для загрузки пакетов, которых не хватает на целевых устройствах, из общедоступных хранилищ в Интернете или корпоративных зеркальных хранилищ в открытой среде. Если происходит ошибка, утилита kdt-airgap-prepare завершает работу и отправляет соответствующее сообщение об ошибке в файл журнала и в стандартный поток вывода (stdout).

Загрузка необходимых пакетов в открытой среде

Чтобы загрузить необходимые пакеты, указанные в файле инвентаря:

1. Скопируйте файл инвентаря YAML на съемный диск, а затем переместите файл на устройство администратора в открытой среде.

2. На устройстве администратора выполните команду. Укажите путь к файлу инвентаря и путь к архиву пакетов, в котором должны быть сохранены недостающие требуемые пакеты:

   ```
   kdt-airgap-preparation pull -n <full_path_to_inventory_file> -a
   <full_path_to_package_archive>
   ```

   Утилита kdt-airgap-preparation загружает пакеты, указанные в файле инвентаря, а также зависящие от них пакеты, и сохраняет пакеты в архиве пакетов TAR. Архив пакетов сохраняется в указанной директории с указанным именем.

3. Добавьте файл инвентаря в архив пакетов.

Созданный архив пакетов будет использован для установки недостающих необходимых пакетов на целевых устройствах в среде с физической изоляцией. Если возникает ошибка, утилита kdt-airgap-prepare завершает работу, выводит соответствующее сообщение об ошибке и записывает ошибку в файл журнала и в stdout.

Установка или обновление пакетов на целевых устройствах в среде с физической изоляцией

Чтобы установить или обновить пакеты и зависящие от них пакеты на целевых устройствах:

1. Скопируйте архив пакетов TAR на съемный диск, а затем переместите архив на устройство администратора в среде с физической изоляцией.

2. На устройстве администратора выполните команду. Укажите путь к архиву пакетов TAR и путь к закрытой части SSH-ключа, который расположен на устройстве администратора и используется для подключения к целевым устройствам:

   ```
   kdt-airgap-preparation install -a <full_path_to_package_archive> -k
   <full_path_to_ssh_key>
   ```

   Утилита kdt-airgap-preparation устанавливает или обновляет требуемые пакеты на целевых устройствах с помощью файла инвентаря и архива пакетов.

После подготовки целевых устройств установите или обновите Kaspersky EDR Expert.

Предварительная проверка готовности инфраструктуры для развертывания

После того как вы начнете развертывание Kaspersky EDR Expert, KDT проверяет, соответствуют ли аппаратное и программное обеспечение, а также сетевая конфигурация узлов кластера Kubernetes необходимым условиям для установки решения. Предварительная проверка выполняется для каждого узла кластера.

Все проверки разделены на две группы:

- Строгие проверки.

  Проверка параметров, которые критически важны для работы Kaspersky EDR Expert. Если эта проверка не пройдет, развертывание прерывается.

- Нестрогие проверки.

  Проверка параметров, которые не являются критически важными для работы Kaspersky EDR Expert. Если эта проверка не пройдена, развертывание продолжается.

Выполняются следующие предварительные проверки:

- Оборудование:
  - На дисках достаточно свободного места для развертывания.
  - Конфигурация процессора соответствует требованиям.
  - Свободного пространства оперативной памяти достаточно для развертывания.
  - Процессор поддерживает инструкции AVX, SSE 4.2 и BMI.
  - Объем свободного места на диске в директории `/tmp` должен быть не меньше размера транспортного архива (строгая проверка для устройства администратора).
- Программное обеспечение:
  - Операционная система и ее версия соответствуют требованиям.
  - Версия ядра соответствует требованиям.
  - Systemctl установлен и доступен (строгая проверка).
  - Доступно обновление кеша диспетчера пакетов (строгая проверка).
  - На узле установлены необходимые пакеты правильной версии (строгая проверка).
  - На узле не установлены запрещенные пакеты (docker и podman) (строгая проверка).
  - Отсутствуют устаревшие бинарные файлы k0s (строгая проверка).

- Отсутствуют устаревшие конфигурационные файлы k0s (строгая проверка).
- Параметры сервера СУБД PostgreSQL или Postgres Pro соответствуют требованиям (строгая проверка).

- Сеть:
  - Все узлы кластера расположены в одном широковещательном домене.
  - Все узлы кластера имеют уникальные имена (параметр `desc` конфигурационного файла) (строгая проверка).
  - Файл пользовательского сертификата действителен для указанного домена и содержит закрытый ключ шифрования (строгая проверка).
  - Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше (строгая проверка).
  - Максимальный срок действия пользовательского конечного сертификата должен быть 399 дней или больше (строгая проверка).
  - На узле доступно разрешение DNS-имен (строгая проверка).
  - На узлах кластера настроена синхронизация времени (строгая проверка).
  - Местное время на всех узлах отличается не более чем на 5 секунд (строгая проверка).
  - Доступны необходимые порты.

Если все строгие предварительные проверки успешно пройдены, KDT разворачивает компоненты Kaspersky EDR Expert в кластере Kubernetes на целевых устройствах. Результаты всех пройденных и не пройденных проверок сохраняются на каждом узле в файле /tmp/k0s_report.txt. Вы можете пропустить предварительные проверки перед развертыванием, если это необходимо (укажите для параметра установки `ignore_precheck` значение `true`).

Проверка целостности компонентов Kaspersky EDR Expert перед установкой

После получения транспортного архива с компонентами Kaspersky EDR Expert вы можете проверить их подлинность и целостность. Каждый компонент (CNAB) в транспортном архиве включает в себя файл манифеста в формате XML. Манифест содержит контрольные суммы компонентов и подписан цифровой подписью с использованием 256-битного алгоритма ГОСТ Р 34.11-2012. Эта цифровая подпись позволяет обеспечить достоверность контрольных сумм файлов компонентов и убедиться, что контрольные суммы в манифесте не были изменены.

Вы можете удостовериться, что контрольные суммы компонентов соответствуют контрольным суммам, указанным в манифестах. Это позволяет подтвердить, что компоненты не были изменены и были получены из доверенного источника.

Чтобы проверить целостность компонентов Kaspersky EDR Expert:

1. Распакуйте транспортный архив.

2. Выполните одну из следующих команд из директории с извлеченными компонентами и их манифестами:

   - Проверка отдельного компонента

     Укажите имя манифеста для проверки соответствующего компонента. Утилита `integrity_checker` проверяет цифровую подпись указанного манифеста:

     ```
     ./integrity_checker --signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     <CNAB_manifest_file.xml>
     ```

   - Проверка всех компонентов

     Утилита `integrity_checker` проверяет цифровые подписи всех манифестов:

     ```
     find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
     signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     ```

Пример вывода команды после успешной проверки целостности

Число манифестов, успешно прошедших проверку, отображается в строке `Manifests` в столбце `succeeded`.

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 38
        Files: 0 / 0 / 38
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
SUCCEEDED
```

Пример вывода команды после неудачной проверки целостности

В этом примере манифест был изменен после подписания или возникла проблема с подписью. Число пропущенных манифестов или манифестов, проверка которых не прошла, отображается в строке `Manifests` в столбце `failed`.

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 2 / 0 / 36
        Files: 0 / 0 / 0
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
FAILED
ERR Can't verify digital signature of file "/home/xdr_user/integrity_check.xml". Flags: None: 0x80000106
(Object is untrusted)
Manifest /home/xdr_user/integrity_check.xml failed. Reason: Can't verify digital signature of file
"/home/xdr_user/integrity_check.xml". Flags: None: 0x80000106 (Object is untrusted)
```

Проверка подлинности и целостности компонентов Kaspersky EDR Expert выполнена.

Вход в Kaspersky EDR Expert

Чтобы войти в Kaspersky EDR Expert, вам нужно знать веб-адрес Консоли OSMP. В вашем браузере JavaScript должен быть включен.

Чтобы войти в Консоль OSMP:

1. В браузере перейдите по адресу `https://<console_host>.<smp_domain>:443`.

   Адрес Консоли OSMP состоит из значений параметров `console_host` и `smp_domain`, указанных в конфигурационном файле.

   Отобразится страница входа в приложение.

2. Выполните одно из следующих действий:

   - Чтобы войти в Консоль OSMP с использованием доменной учетной записи пользователя, введите имя пользователя и пароль доменного пользователя.

     Вы можете ввести имя доменного пользователя в одном из следующих форматов:

     - `Username@dns.domain`
     - NTDOMAIN\`Username`.

   - Введите имя пользователя и пароль внутреннего пользователя.

3. Нажмите на кнопку **Войти**.

4. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

   При первом входе настройте двухэтапную аутентификацию для своей учетной записи. Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и который настроил двухфакторную аутентификацию, чтобы добавить вашу учетную запись в список пользователей с правом настраивать двухфакторную аутентификацию.

5. Если для вашей учетной записи включено принудительное изменение пароля или срок действия пароля истек, отобразится окно изменения пароля. Установите новый пароль для входа в Консоль OSMP.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз.

Превышено разрешенное количество попыток входа в систему

В дистрибутив OSMP входит правило корреляции *[OOTB] Multiple login attempts to OSMP console using the same account*. Это правило добавляется в коррелятор, который устанавливается при развертывании OSMP. Это правило предусматривает создание события корреляции после трех неудачных попыток входа пользователя в Консоль OSMP.

На основе сгенерированного события корреляции создается алерт о превышении разрешенного количества попыток входа в систему.

Вы можете изменить допустимое количество попыток ввода пароля. Подробнее см. в статье Изменение количества попыток ввода пароля.

Доменная аутентификация

Kaspersky EDR Expert позволяет использовать доменную аутентификацию по протоколу Kerberos. Дополнительные сведения см. в статье Настройка доменной аутентификации Kerberos.

Чтобы выйти из Консоли OSMP,

в верхней панели откройте меню своей учетной записи, нажав на ее имя, и выберите **Выход**.

Консоль OSMP закрыта и отображается страница входа в приложение.

Интеграция с Endpoint Agent

Чтобы интегрировать Endpoint Agent, вам нужно получить сертификаты, необходимые для создания *доверенного соединения* между OSMP и Endpoint Agent.

Чтобы получить сертификат для приема телеметрии от Endpoint Agent:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. В списке сервисов в контекстном меню коллектора, который вы хотите использовать для сбора телеметрии от агентов Endpoint Agent, выберите пункт **Скачать сертификат**.

   Ваш браузер загружает TLS-сертификат сервера в папку загрузок.

Чтобы получить сертификат для отправки реагирования в Endpoint Agent:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**, нажмите на название тенанта и выберите вкладку **Параметры** → **Сертификаты**.
2. В разделе **Сертификат Сервера** нажмите **Экспорт**.

   Ваш браузер загружает TLS-сертификат сервера в папку загрузок.

Чтобы получить TLS-сертификат Endpoint Agent:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**, нажмите на название тенанта и выберите вкладку **Параметры** → **Сертификаты**.
2. В разделе **Агенты Endpoint Agent** выберите текущий сертификат TLS и нажмите **Экспорт**.
3. Укажите пароль для PFX-архива защищенного паролем, содержащего TLS-сертификат агентов Endpoint Agent, и нажмите на кнопку **Экспорт**.

   Ваш браузер загружает PFX-архив (криптоконтейнер) в папку загрузок.

   Полученный сертификат требуется для взаимной TLS-аутентификации при отправке реагирования Endpoint Agent и получения телеметрии.

После того как вы скачали все необходимые сертификаты, вы можете создать политику для интеграции Endpoint Agent. Подробные инструкции по созданию политики и добавлению сертификатов см. в документации Endpoint Agent:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Подготовка и установка Sandbox

Чтобы подготовиться к установке и установить Sandbox:

1. Подготовьте ИТ-инфраструктуру к установке Sandbox.
2. Подготовьте виртуальную машину.
3. Подготовьте образ установочного диска.
4. Установите Sandbox.

Подготовка ИТ-инфраструктуры к установке Sandbox

Чтобы подготовить ИТ-инфраструктуру к установке Sandbox:

1. Запретите доступ к локальной сети сервера Sandbox для интерфейса управления сетью и интерфейса сети, используемого для доступа в интернет обрабатываемых объектов.
2. Укажите порты для взаимодействия с другими компонентами следующим образом:
   - Входящее направление (управляющий интерфейс)
     - TCP 22

       Подключение к серверу по протоколу SSH
     - TCP 443

       Взаимодействие с OSMP.
     - TCP 8443

       Доступ к веб-интерфейсу приложения
   - Исходящее направление (управляющий интерфейс)
     - TCP 80 или TCP 443

       Связь с серверами обновлений "Лаборатории Касперского".
   - Исходящие и соответствующие входящие направления (интерфейс для доступа к обрабатываемым объектам):

Любой порт.

Доступ в сеть интернет для анализа сетевого поведения исследуемых объектов.

Доступ запрещен к корпоративной локальной сети для защиты сети от анализируемых объектов.

Подготовка виртуальной машины к установке Sandbox

Чтобы подготовить виртуальную машину к установке компонента Sandbox:

1. Запустите гипервизор VMware ESXi.
2. Откройте консоль управления виртуальной машиной.
3. В контекстном меню виртуальной машины, на которую вы хотите установить компонент Sandbox, выберите **Изменить параметры**.

   Откроется окно свойств виртуальной машины.
4. На вкладке **Virtual Hardware** разверните группу параметров CPU и установите флажок **Expose hardware-assisted virtualization to guest OS**.
5. На вкладке **VM Options** в раскрывающемся списке **Latency Sensitivity** выберите **High**.
6. Нажмите на кнопку **OK**.

Виртуальная машина будет готова к установке компонента Sandbox.

Подготовка образа установочного диска

Перед установкой Sandbox необходимо подготовить образ ISO установочного диска на базе операционной системы Astra Linux.

Минимальные аппаратные требования для устройства, которое можно использовать для создания образа ISO:

- Процессор: 4 ядра, тактовая частота 2500 МГц или больше.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 100 ГБ.

Программные требования:

- Операционная система на базе актуального ядра Linux.
- Docker 20 и выше.
- Наличие iso-образа операционной системы Astra Linux Special Edition версии 1.8.2.8 (далее этот образ упоминается под именем astra-installation.iso).

Kaspersky EDR Expert не поддерживает другие версии операционной системы Astra Linux.

Чтобы смонтировать iso-образ компонента Sandbox на базе операционной системы Astra Linux:

1. Скачайте следующие файлы из дистрибутива:
   - Архив tar.gz из дистрибутива Sandbox.
   - Инструменты для создания образа ISO.
2. Создайте файл iso_builder.sh со следующим содержимым:

```
#!/bin/bash

usage="Builds the KEDR install ISO.

Usage:

$(basename "$0") [-h] source_iso distribution iso_builder_image build target_iso_name

где:
    -h, --help        - show this text and exit
    source_iso        - absolute path to the source OS ISO file
    distribution      - absolute path to the KEDR distribution archive
    iso_builder_image - absolute path to the iso_builder docker image
    build             - absolute path to a temporary build directory
    target_iso_name   - absolute path to the resulting ISO file
"

if [ "$#" -eq 0 ] || [ "$1" == "-h" ] || [ "$1" == "--help" ]
then
    echo "$usage"; exit 10;
fi

if [ "$#" -lt 5 ]
then
    echo "Error: not enough arguments. Please, refer the help text."; exit 11;
fi

docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --source-iso-uri file://$1
--kata-distribution-uri file://$2 --target-iso-name $5
```

3. Выполните следующую команду:

```
mkdir /var/kedr_builder
```

4. Поместите файлы, перечисленные в шаге 1, и образ astra-installation.iso в созданную директорию /var/kedr_builder.
5. Выполните следующую команду:

```
sudo ./iso_builder.sh \
 /var/kedr_builder/astra-installation.iso \
 /var/kedr_builder/kata-sb-distribution-<версия>-x86_64_en-ru-zh.tar.gz \
 /var/kedr_builder/iso-builder-<версия>-x86_64_en-ru-zh.tar \
 /var/kedr_builder buildSandboxAstra.iso
```

   где <версия> – версия дистрибутива Sandbox.

   Образ установочного диска buildSandboxAstra.iso создается в директории /var/kedr_builder.

Если вы храните файлы в разных директориях, вы можете выполнить следующую команду:

```
sudo ./iso_builder.sh <source_iso_host_path> <distribution_host_path> <iso_builder_image_host_path>
<build_host_path> <target_iso_name>
```

В приведенной выше команде:

- source_iso_host_path – путь к дистрибутиву Astra Linux Special Edition 1.8.2.8.
- distribution_host_path – путь к дистрибутиву Sandbox.
- iso_builder_image_host_path – путь к инструменту создания ISO.
- build_host_path – путь, по которому должен находиться смонтированный образ ISO, без указания имени, которое будет присвоено образу ISO.
- target_iso_name – это имя, присвоенное образу ISO.

Установка Sandbox

Чтобы начать установку компонента Sandbox:

1. Запустите образ диска, содержащий компонент Sandbox.

   Запустится мастер установки.

2. Выберите **Продолжить** и нажмите на клавишу **`Enter`**.

Шаг 1. Ознакомление с Лицензионным соглашением и Политикой конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

В операционной системе Astra Linux вам также нужно принять Лицензионное соглашение операционной системы Astra Linux.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **`Enter`**.

2. В операционной системе Astra Linux вам сначала нужно принять Лицензионное соглашение операционной системы Astra Linux. Прочтите Лицензионное соглашение. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **`Enter`**.

3. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского". Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **`Enter`**.

4. Прочтите Политику конфиденциальности. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки Sandbox

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **`Enter`**.

2. В окне подтверждения выберите **Yes** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Настройка минимальной длины пароля администратора Sandbox

Чтобы задать минимальную длину пароля администратора компонента Sandbox:

1. В поле **Минимальная длина пароля** введите количество символов.

   Рекомендуется использовать пароли длиной 12 и более символов.

2. Выберите **OK** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Создание учетной записи администратора Sandbox

Чтобы создать учетную запись администратора Sandbox:

1. В поле **Новое имя пользователя** введите имя учетной записи администратора. По умолчанию используется учетная запись admin.

2. В поле **Новый пароль** введите пароль учетной записи администратора.

   Пароль должен соответствовать следующим правилам:

   - Пароль должен содержать минимум 8 символов.

   - Пароль должен содержать символы минимум трех типов:

     - символ верхнего регистра (A-Z);

     - символ нижнего регистра (a-z);

     - цифру;

     - специальный символ.

- Пароль не должен полностью или в значительной части совпадать с именем пользователя.
- Пароль не должен содержать три и более одинаковых символов подряд.

3. В поле **Подтвердить пароль** введите пароль повторно.
4. Выберите **OK** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Настройка управляющего сетевого интерфейса

Для работы компонента Sandbox необходимо подключить минимум две сетевые карты и настроить следующие сетевые интерфейсы:

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для доступа к серверу Sandbox по протоколу SSH, а также через этот интерфейс сервер Sandbox будет принимать объекты для проверки.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает Sandbox, смогут предпринимать попытки действий в интернете, а Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

> Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего и настройте его параметры.

Чтобы выбрать управляющий сетевой интерфейс и настроить его параметры:

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
2. Нажмите на клавишу **`Enter`**.
3. В поле **Адрес** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска сети** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Выберите **OK** и нажмите на клавишу **`Enter`**.
6. Выберите **Продолжить** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Назначение имени устройства и добавление адресов DNS-серверов

Назначьте имя устройства сервера для использования DNS-серверами и добавьте адреса DNS-серверов.

Чтобы назначить имя устройства сервера и добавить адреса DNS-серверов:

1. В окне **Параметры DNS** выберите пункт **Имя устройства**.
2. В поле **Имя устройства** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).
3. Выберите **OK** и нажмите на клавишу **`Enter`**.
4. В окне **DNS settings** выберите пункт **DNS servers**.
5. Выберите **New** и нажмите на клавишу **`Enter`**.

   Откроется окно ввода адреса DNS-сервера.
6. В поле **DNS-сервер** введите IP-адрес основного DNS-сервера в формате IPv4.
7. Выберите **OK** и нажмите на клавишу **`Enter`**.

   Окно ввода адреса DNS-сервера закроется.
8. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите шаги 5–7 этой инструкции для каждого сервера, который вы хотите добавить.
9. Когда вы добавите все DNS-серверы, выберите **Go back** и нажмите на клавишу **`Enter`**.
10. В окне DNS-серверы выберите **Продолжить** и нажмите на клавишу **`Enter`**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка статического сетевого маршрута

Чтобы настроить статический сетевой маршрут:

1. В окне **IPv4 Routes** выберите **New** и нажмите на клавишу **`Enter`**.

   Откроется окно **IPv4 Static Route**.
2. В поле **Адрес/Маска** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
3. Если вы хотите использовать сетевой маршрут по умолчанию, введите **`0.0.0.0/0`**.
4. В поле **Шлюз соединения** введите IP-адрес шлюза.
5. Выберите **OK** и нажмите на клавишу **`Enter`**.
6. Если вы хотите добавить другие сетевые маршруты, повторите шаги 1–5 этой инструкции для каждого сетевого маршрута, который вы хотите добавить.
7. Когда вы закончите добавлять сетевые маршруты, нажмите на кнопку **Продолжить**.

Настройка займет некоторое время. После этого установка завершится.

Интеграция с Kaspersky Sandbox

Интеграция с Sandbox состоит из двух шагов:

1. Создание запроса на подключение к серверу Sandbox в интерфейсе OSMP.

2. Подтверждение запроса в веб-интерфейсе Sandbox.

Чтобы создать запрос на подключение к серверу Sandbox через интерфейс OSMP:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** перейдите в раздел **Серверы Sandbox**.

   Обратите внимание на *отпечаток сертификата OSMP*. Этот отпечаток потребуется позже, он должен совпадать с отпечатком, отображаемым в веб-интерфейсе Sandbox.

4. Нажмите на кнопку **Добавить**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить сервер Sandbox**.

5. В поле **IP** укажите IP-адрес сервера Sandbox.

6. Нажмите **Получить отпечаток сертификата**. Kaspersky EDR Expert отображает *отпечаток сертификата Sandbox*. Этот отпечаток потребуется позже, он должен совпадать с отпечатком, отображаемым в веб-интерфейсе Sandbox.

7. В поле **Название Sandbox** укажите имя компонента Sandbox, которое будет отображаться в интерфейсе OSMP.

8. Нажмите на кнопку **Сохранить**.

OSMP отправляет запрос на подключение к Sandbox. Теперь вам нужно подтвердить запрос.

Чтобы подтвердить запрос на подключение от OSMP:

1. В веб-интерфейсе Sandbox перейдите в раздел **Авторизация**.

2. Сравните отпечатки сертификатов:

   - Отпечаток сертификата Sandbox, отображаемый под IP-адресом Sandbox, должен совпадать с отпечатком сертификата Sandbox, полученным ранее в интерфейсе OSMP.

   - В списке запросов на подключение от OSMP найдите запрос на подключение из Консоли OSMP. Столбец **Отпечаток сертификата** содержит отпечаток сертификата сервера OSMP, отправившего запрос на подключение. Этот отпечаток сертификата должен совпадать с отпечатком сертификата OSMP, полученным ранее в интерфейсе OSMP.

3. Чтобы подтвердить запрос на подключение, нажмите **Принять**. Позже вы можете отозвать ранее принятый запрос на подключение, нажав на кнопку **Отозвать**.

4. Нажмите на кнопку **Применить**.

Интеграция с Sandbox настроена.

Развертывание Kaspersky EDR Expert с высокой доступностью

В этом разделе описывается порядок развертывания Kaspersky EDR Expert на четырех серверах (см. также расчеты масштабирования). Подобная конфигурация не гарантирует полную отказоустойчивость, она достаточно надежна и допускает развертывание с минимальным бюджетом.

Используя этот сценарий, вы можете подготовить свою инфраструктуру для развертывания Open Single Management Platform и всех необходимых компонентов Kaspersky EDR Expert в отказоустойчивой конфигурации. Вы также можете подготовить конфигурационный файл с параметрами установки и развернуть решение с помощью утилиты Kaspersky Deployment Toolkit (далее KDT).

> Прежде чем приступить к развертыванию Open Single Management Platform и компонентов Kaspersky EDR Expert, рекомендуется ознакомиться с Руководством по усилению защиты.

Сценарий развертывания состоит из следующих этапов:

1. **Скачать дистрибутив с компонентами Kaspersky EDR Expert**

   В дистрибутив входят:

   - Транспортный архив, который содержит компоненты Kaspersky EDR Expert, Лицензионное соглашение для Kaspersky EDR Expert и Лицензионное соглашение для KDT.
   - Архив с утилитой KDT, а также шаблоны конфигурационного файла и файла инвентаря KUMA.

2. **Установить систему управления базами данных (СУБД)**

   Вручную установите СУБД на отдельных серверах, которые не будут включены в кластер Kubernetes.

   Используйте одну из поддерживаемых конфигураций баз данных высокой доступности: Отказоустойчивая конфигурация Kaspersky EDR Expert.

3. **Подготовить устройство администратора и целевые устройства**

   Определите число целевых устройств, на которых будут развернуты кластер Kubernetes и компоненты Kaspersky EDR Expert. В отказоустойчивой конфигурации Kaspersky EDR Expert должно быть не менее четырех целевых устройств.

   Подготовьте устройство администратора и целевые устройства к развертыванию.

   Инструкция: Развертывание на нескольких узлах –подготовка устройства администратора и целевых устройств.

4. **Подготовить конфигурационный файл**

   Создайте конфигурационный файл в формате YAML. Этот файл содержит список целевых устройств для развертывания и параметры установки компонентов Kaspersky EDR Expert.

Инструкция: Развертывание на нескольких узлах – параметры установки.

Вы можете заполнить файл вручную или воспользоваться мастером настройки, чтобы указать параметры установки и создать файл автоматически.

Инструкция: Указание параметров установки с помощью мастера настройки.

5. **Развертывание Kaspersky EDR Expert**

   Разверните решение с помощью KDT. Инструмент автоматически настраивает кластер Kubernetes и устанавливает компоненты Kaspersky EDR Expert вместе с необходимой инфраструктурой.

   Инструкция: Установка Kaspersky EDR Expert

6. **Установить службы KUMA внутри кластера Kubernetes**

   Разверните службы KUMA (коллекторы, корреляторы и хранилища).

   Инструкция: Установка служб KUMA внутри кластера Kubernetes.

7. **Добавить подчиненный Сервер администрирования**

   Подчиненный Сервер администрирования требуется для дальнейшей интеграции с Endpoint Agent.

   Рекомендуется использовать подчиненный Сервер администрирования – при подобном подходе указаны четкие требования к оборудованию для работы с нагрузкой. Это позволяет более точно планировать и настраивать инфраструктуру, чтобы обеспечить оптимальную производительность и эффективность.

   Инструкция: Добавление подчиненного Сервера администрирования.

8. **Установить и интегрировать агенты Endpoint Agent**

   Установите агенты Endpoint Agent в соответствии с документацией:

   - Kaspersky Endpoint Security для Windows
   - Kaspersky Endpoint Security для Linux
   - Kaspersky Endpoint Security для Mac

   Настройте интеграцию с Endpoint Agent.

9. **Установить и интегрировать Sandbox**

   Установите и настройте Sandbox, затем разверните в ней необходимые виртуальные машины. После этого настройте интеграцию с Sandbox.

   Инструкции:

   - Установка компонента Sandbox
   - Первоначальная настройка Sandbox
   - Подготовка виртуальных машин к работе
   - Интеграция с Kaspersky Sandbox

Отказоустойчивая конфигурация Kaspersky EDR Expert

Отказоустойчивая конфигурация позволяет развернуть решение с минимальным бюджетом. Впрочем, это зависит от доступности единственного управляющего узла. Если рабочий узел выходит из строя, производительность упадет. Если из строя выйдет управляющий узел, управление будет недоступно, но сервисы на рабочих узлах продолжат действовать.

Для этой конфигурации требуется как минимум четыре узла кластера Kubernetes:

- 1 управляющий узел (контроллер)
- 3 рабочих узла.

Поддерживаются следующие отказоустойчивые конфигурации СУБД:

- Кластер Postgres Pro Enterprise BiHA
  - Версия: Postgres Pro Enterprise 16 или более поздняя
  - Тип кластера: BiHA
  - Количество узлов: от 3 до 15
  - Тип репликации: синхронная.
  - Строка подключения для доступа к СУБД включает список узлов кластера (задается параметром `psql_dsn`):

    ```
    psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>
    ```

- Кластер PostgreSQL с виртуальным IP-адресом (Corosync/Pacemaker)
  - Тип кластера: Кластер PostgreSQL с виртуальным IP-адресом (Corosync/Pacemaker)
  - Количество узлов: 3 или более
  - Строка подключения для доступа к СУБД включает виртуальный IP-адрес кластера СУБД (задается параметром `psql_dsn`):

    ```
    psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
    ```

Поддерживается следующая отказоустойчивая конфигурация сервисов KUMA, устанавливаемых внутри кластера Kubernetes:

- Хранилище KUMA
  - Количество рабочих узлов: 3 или более.
  - Хранилища KUMA привязаны к этим узлам и не должны переноситься на другие узлы.
  - Хранилища KUMA используют диски этих узлов напрямую, не полагаясь на Longhorn.

- Ядро KUMA
  - Количество рабочих узлов: 1

    Отказоустойчивость обеспечивается Kubernetes. В случае отказа узла время простоя составляет около 6 минут.
- Коллектор KUMA

  Возможны два варианта отказоустойчивой конфигурации:
  - Количество рабочих узлов: 2.

    Минимальное время простоя в случае отказа узла.
  - Количество рабочих узлов: 1.

    Отказоустойчивость обеспечивается Kubernetes. В случае отказа узла время простоя составляет около 6 минут.
- Коррелятор KUMA
  - Количество рабочих узлов: 1.

    Отказоустойчивость обеспечивается Kubernetes. В случае отказа узла время простоя составляет около 6 минут.
- Метрики KUMA
  - Количество рабочих узлов: 1.

    Отказоустойчивость обеспечивается Kubernetes. В случае отказа узла время простоя составляет около 6 минут.

Восстановление отказавшего узла в кластере Kubernetes

Если в узле кластера Kubernetes произошел сбой питания или сети, но данные на его диске остались нетронутыми и его сетевое имя не изменилось, администратору требуется восстановить питание и сетевое подключение. Приблизительно через 5–6 минут после восстановления работоспособности узла он автоматически воссоединяется с кластером.

Если после сбоя данные на диске узла были повреждены или утрачены либо его имя хоста изменилось, узел требуется повторно настроить и подготовить к работе в рамках кластера Kubernetes, а затем повторно добавить в кластер.

Чтобы подготовить и добавить узел в кластер Kubernetes, выполните следующие действия:

1. Подготовьте целевые устройства, которые будут выполнять роль управляющих и рабочих узлов.
2. На устройстве администратора экспортируйте текущий конфигурационный файл с помощью следующей команды:

   ```
   ./kdt ec -e '<имя_конфигурационного_файла_и_путь>'
   ```

   Текущая версия конфигурационного файла сохраняется в указанной директории под указанным именем.

3. В разделе `nodes` экспортированного конфигурационного файла удалите параметры отказавшего узла, затем добавьте параметры восстановленного узла (`desc`, `type`, `host`, `kind`, `user` и `key`). Сохраните обновленный конфигурационный файл.

4. Скопируйте открытый ключ на каждый новый узел (например, в директорию `~/.ssh`) с помощью утилиты ssh-copy-id.

5. Чтобы применить измененный конфигурационный файл к кластеру Kubernetes, выполните следующую команду на хосте администратора, указав полный путь к файлу конфигурации:

   ```
   ./kdt apply -i '<полный_путь_к_конфигурационному_файлу>'
   ```

   После выполнения KDT проверяет конфигурационный файл. Далее он проверяет, соответствует ли аппаратное и программное обеспечение, а также сетевая конфигурация узлов кластера Kubernetes необходимым условиям для установки решения. Если все строгие предварительные проверки пройдены успешно, KDT выводит соответствующее уведомление в stdout и журналы KDT. В противном случае сохраняются журналы с информацией о неудачной проверке и процесс добавления новых устройств прерывается. При необходимости вы можете пропустить предварительную проверку перед запуском команды, указав для параметра установки `ignore_precheck` значение `true`.

Восстановленный узел будет добавлен в кластер Kubernetes. Затем KDT выводит информацию о восстановленном узле в stdout и в журналы KDT.

Развертывание в нескольких ЦОД Kaspersky EDR Expert с высокой доступностью

Развертывание в нескольких ЦОД с отказоустойчивой конфигурацией Kaspersky EDR Expert обеспечивает отказоустойчивость за счет распределения узлов кластера Kubernetes по нескольким центрам обработки данных. Если центр обработки данных становится недоступным, рабочая нагрузка автоматически переносится на узлы кластера в другом центре обработки данных, что позволяет Kaspersky EDR Expert продолжить работу с минимальными сбоями.

Для конфигурации в нескольких ЦОД требуется минимум три центра обработки данных. Развертывание Kaspersky EDR Expert как минимум в трех центрах обработки данных гарантирует сохранение кворума Kubernetes, если один из центров обработки данных становится недоступным. В каждом центре обработки данных необходимо развернуть как минимум четыре узла кластера: один управляющий узел и три рабочих узла. Каждый центр обработки данных использует собственный шлюз кластера Kubernetes с выделенным IP-адресом. Целевые устройства и шлюз кластера Kubernetes должны находиться в одной подсети одного центра обработки данных.

В каждом центре обработки данных требуется хотя бы одно устройство Sandbox. Трафик должен распределяться между узлами кластера в разных центрах обработки данных с помощью управляемой заказчиком высокодоступной балансировщика нагрузки. Вы также должны установить СУБД в поддерживаемой конфигурации высокой доступности.

Например, в конфигурации в нескольких ЦОД с тремя центрами обработки данных должно быть не менее 15 узлов:

- 12 целевых устройств включены в кластер Kubernetes:
  - 3 управляющих узла (не менее 1 узла на каждый центр обработки данных).
  - 9 рабочих узлов (не менее 3 узлов на каждый центр обработки данных).
- 3 устройства Sandbox (не менее 1 узла на каждый центр обработки данных).

Также для развертывания требуются управляемый заказчиком отказоустойчивый балансировщик нагрузки и СУБД, развернутые в поддерживаемой конфигурации отказоустойчивости.

Ограничения развертывания в нескольких ЦОД

- Каналы связи между центрами обработки данных должны обеспечивать пропускную способность не менее 10 Гбит/с и задержку не более 20 мс. Однако рекомендуется использовать каналы связи с пропускной способностью не менее 25 Гбит/с и задержкой не более 5 мс.
- Расстояние между какими-либо двумя центрами обработки данных не должно превышать 800 км. Допустимое расстояние между центрами обработки данных определяется задержкой компонентов, использующих синхронную репликацию, при которой задержка не должна превышать 20 мс.
- Сетевое подключение между узлами в разных центрах обработки данных должно быть установлено через порты, используемые Kaspersky EDR Expert.
- В одном центре обработки данных (зоне) все узлы должны находиться в одном сегменте L2 (широковещательном домене).
- База данных PostgreSQL должна быть развернута в отказоустойчивой конфигурации с синхронной репликацией, а посредник должен находиться в другой зоне, чтобы обеспечить оптимальную производительность и избыточность.
- Внешний балансировщик нагрузки предоставляется заказчиком.
- Ручной обход отказа Endpoint Agents между центрами обработки данных не поддерживается.
- Репликация с использованием Patroni должна быть синхронной.
- Репликацию данных телеметрии между центрами обработки данных необходимо настраивать вручную с помощью инструментов ClickHouse.

Известные проблемы при сбоях центров обработки данных

- Файлы, которые Anti-Malware Engine отправляет на проверку в Sandbox, могут быть потеряны в случае недоступности центра обработки данных, в котором размещается Sandbox. Кроме того, при автоматической проверке в Sandbox также могут возникать задержки.
- Могут быть потеряны задачи IRP, включая задачи проверки, которые выполнялись в центре обработки данных на момент наступления недоступности. Для этих задач не будут получены результаты обнаружения.
- В случае недоступности некоторых центров обработки данных, в которых размещается Sandbox, оставшиеся ЦОД могут испытывать повышенную нагрузку из-за заполнения очередей во внешних системах. В результате по мере роста числа запросов на обработку в Sandbox может происходить отбрасывание задач.
- Если файлы, отправленные на проверку в определенный центр обработки данных, не удается обработать из-за недоступности этого ЦОД, результаты проверки (обнаружения) по этим файлам утрачиваются, а сами файлы по умолчанию помечаются как "безопасные". Потеря файлов и обнаружений может продолжаться до 15 минут, если требования к масштабированию Sandbox удовлетворяются, и до 1 часа в противном случае.
- После восстановления центра обработки данных или его добавления для создания развертывания в нескольких ЦОД решению может потребоваться 30–60 минут, чтобы стать отказоустойчивым, пока данные кластера будут синхронизированы. В это время решение работает нормально, но может стать недоступным, если один из центров обработки данных перейдет в автономный режим. Синхронизация может занять больше времени, если объемы данных больше размера по умолчанию. Низкая пропускная способность или высокая задержка между центрами обработки данных также могут увеличить время синхронизации.

Этапы

Следуя этому сценарию, вы можете подготовить инфраструктуру к развертыванию Open Single Management Platform и всех необходимых компонентов для Kaspersky EDR Expert в нескольких центрах обработки данных, подготовить конфигурационный файл, содержащий параметры установки, и развернуть решение с помощью утилиты Kaspersky Deployment Toolkit (далее также KDT).

> Прежде чем приступить к развертыванию Open Single Management Platform и компонентов Kaspersky EDR Expert, рекомендуется прочитать Руководство по усилению защиты.

Сценарий развертывания состоит из следующих этапов:

1. **Загрузка дистрибутива с компонентами Kaspersky EDR Expert**

В состав дистрибутива входят следующие компоненты:

- Транспортный архив, который содержит компоненты Kaspersky EDR Expert и Лицензионные соглашения Kaspersky EDR Expert и KDT.

  Компоненты подписаны ключом RSA и ключом ГОСТ Р 34.11-2012. Вы можете проверить подлинность и целостность компонентов Kaspersky EDR Expert.

- Архив с утилитой KDT, а также шаблоны конфигурационного файла и файл инвентаря KUMA.

2. **Установка системы управления базами данных (СУБД)**

Вручную установите СУБД на отдельные серверы в одной из поддерживаемых отказоустойчивых конфигураций СУБД: Отказоустойчивая конфигурация Kaspersky EDR Expert.

СУБД предоставляется и настраивается заказчиком.

3. **Настройка отказоустойчивого балансировщика нагрузки**

Настройте отказоустойчивый балансировщик нагрузки для распределения входящего трафика между узлами кластера, расположенными в нескольких центрах обработки данных.

Балансировщик нагрузки предоставляется и настраивается заказчиком.

Пример файла конфигурации

Например, вы можете использовать HAProxy с открытым исходным кодом в качестве балансировщика нагрузки. Укажите IP-адрес шлюза кластера Kubernetes (параметр `ingress_ip` в конфигурационном файле) для каждого центра обработки данных в конфигурации балансировщика нагрузки.

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
        daemon

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http

listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST

frontend http
  mode tcp
```

```
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:80 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:80 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:80 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway

frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway

frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:9443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:9443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:9443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway

frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:4443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:4443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:4443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway

frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:13000 check inter 5s # first data center - IP address of the Kubernetes
```

```
cluster gateway
  server proxmox2 <ingress_ip_2>:13000 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:13000 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
```

4. **Подготовка устройства администратора и целевых устройств**

   Определите количество целевых устройств, на которых будет развернут кластер Kubernetes и компоненты Kaspersky EDR Expert, в каждом центре обработки данных, а затем подготовьте устройство администратора и целевые устрйоства для развертывания Kaspersky EDR Expert.

   Если вы выполняете развертывание в нескольких ЦОД, вы также должны настроить записи DNS таким образом, чтобы FQDN служб разрешались в IP-адрес балансировщика нагрузки, управляемого заказчиком.

   Инструкция: Развертывание в нескольких ЦОД: подготовка устройства администратора и целевых устройств

5. **Подготовка устройств KUMA для установки сервисов KUMA вне кластера Kubernetes (не обязательно)**

   Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера Kubernetes, на отдельных хостах вне кластера или частично в кластере и вне его.

   Если вы хотите полностью установить сервисы KUMA на отдельных устройствах вне кластера Kubernetes или частично в кластере и вне его, вам потребуется подготовить целевые устройства KUMA к установке сервисов KUMA.

   Инструкция: Подготовка устройств KUMA к установке сервисов KUMA вне кластера Kubernetes

6. **Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes (не обязательно)**

   Если вы хотите полностью установить сервисы KUMA на отдельных устройствах вне кластера Kubernetes или частично в кластере и вне его, вам потребуется подготовить файл инвентаря KUMA в формате YAML. Файл инвентаря KUMA содержит параметры для установки сервисов KUMA вне кластера Kubernetes.

   Инструкция: Подготовка файла инвентаря KUMA для установки сервисов KUMA вне кластера Kubernetes

7. **Подготовка конфигурационного файла**

   Подготовьте конфигурационный файл в формате YAML. Конфигурационный файл содержит список целевых устройств для развертывания и набор параметров для установки компонентов Kaspersky EDR Expert.

   Если вы выполняете развертывание в нескольких ЦОД, вы также должны указать параметры регионов инфраструктуры и центров обработки данных.

   Инструкция: Развертывание в нескольких ЦОД: параметры установки

8. **Развертывание Kaspersky EDR Expert**

   Разверните Kaspersky EDR Expert с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Kaspersky EDR Expert и другие компоненты инфраструктуры.

   Инструкции: Установка Kaspersky EDR Expert.

9. **Установка сервисов KUMA**

   Установите сервисы KUMA (коллекторы, корреляторы и хранилища).

   Сервисы KUMA можно установить полностью внутри кластера Kubernetes, полностью на отдельных узлах вне кластера или частично внутри и частично вне кластера Kubernetes.

   Инструкция: Установка сервисов KUMA вне кластера Kubernetes

   Инструкция: Установка сервисов KUMA внутри кластера Kubernetes

10. **Добавление подчиненного Сервера администрирования**

    Подчиненный Сервер администрирования требуется для дальнейшей интеграции с Endpoint Agent.

    Инструкции: Добавление подчиненного Сервера администрирования.

11. **Установка и интеграция с Endpoint Agent**

    Установите Endpoint Agent в соответствии с документацией к Endpoint Agent:

    - Kaspersky Endpoint Security для Windows
    - Kaspersky Endpoint Security для Linux
    - Kaspersky Endpoint Security для Mac

    Настройте интеграцию с Endpoint Agent.

12. **Установка и интеграция с Sandbox**

    Установите Sandbox, настройте Sandbox и установите виртуальные машины в Sandbox.

    Настройте интеграцию с Sandbox.

Развертывание в нескольких ЦОД: подготовка устройства администратора и целевых устройств

Подготовка к развертыванию в нескольких центрах обработки данных (ЦОД) включает настройку устройства администратора и целевых устройств. После подготовки устройств и указания конфигурационного файла вы сможете развернуть Kaspersky EDR Expert на целевых устройствах с использованием KDT.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям.

   Если устройство администратора не входит в кластер Kubernetes, обратитесь к требованиям KDT.

   Если устройство администратора входит в кластер, обратитесь к требованиям к оборудованию для развертывания на нескольких узлах и к программным требованиям OSMP.

2. Выделите не менее 15 ГБ свободного места в директории временных файлов (по умолчанию `/tmp`) для KDT. Если у вас недостаточно свободного места в этой директории, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<новая_директория>/tmp
   ```

3. Настройте среду выполнения контейнера. Используйте одну из следующих сред выполнения контейнеров:

   - Встроенная среда выполнения контейнера KDT (на основе runc).

     Выполните команду, чтобы установить встроенную среду выполнения контейнера:

     ```
     sudo ./kdt init
     ```

     Если встроенная среда выполнения контейнера не подходит, вы можете использовать вместо нее среду выполнения контейнера Docker.

   - Среда выполнения контейнера Docker.

     Установите пакет для Docker версии 25 или выше, а затем выполните действия после установки, чтобы настроить устройство администрирования для правильной работы с Docker.

     На разделе диска для хранения данных Docker (по умолчанию `/var/lib/docker`) должно быть не менее 60 ГБ свободного места.

     Не устанавливайте неофициальные версии пакета Docker из хранилищ операционных систем.

4. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Поскольку устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на нескольких узлах.

   b. Убедитесь, что на устройстве администратора поддерживается технология cgroup v2.

Подготовка целевых устройств

Целевые устройства – это физические или виртуальные машины, которые используются для развертывания Kaspersky EDR Expert и которые включены в кластер Kubernetes. Компоненты Kaspersky EDR Expert работают на этих устройствах.

> Одно из целевых устройств может быть использовано в качестве устройства администратора. В этом случае вам необходимо подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, а затем подготовить целевое устройство.

Для конфигурации в нескольких ЦОД с тремя центрами обработки данных должно быть не менее 12 узлов кластера:

- 3 управляющих узла (не менее 1 узла на каждый центр обработки данных).

  Управляющий узел предназначен для управления кластером, хранения метаданных и распределения рабочей нагрузки.

- 9 рабочих узлов (не менее 3 узлов на каждый центр обработки данных).

  Рабочие узлы предназначены для выполнения рабочей нагрузки компонентов Kaspersky EDR Expert.

Количество первичных и рабочих узлов в кластере может быть разным. Для оптимального распределения нагрузки между узлами рекомендуется использовать узлы с примерно одинаковой производительностью.

Службы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на рабочих узлах, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его.

Чтобы подготовить целевые устройства:

1. Убедитесь, что оборудование и программное обеспечение на целевых устройствах соответствуют требованиям для развертывания на нескольких узлах и целевые устройства расположены в одном широковещательном домене.

   Если сервисы KUMA установлены внутри кластера, целевые устройства должны соответствовать требованиям к оборудованию, программному обеспечению и требованиям к установке, необходимым для установки сервисов KUMA.

   > Для правильной работы Kaspersky EDR Expert версия ядра Linux должна быть 5.15.0.107 или выше на целевых устройствах с операционной системой семейства Ubuntu.

   > Docker не должен быть установлен на целевых устройствах, кроме целевого устройства, которое будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. Убедитесь, что в файловой системе, смонтированной в `/var`, на каждом целевом устройстве есть не менее 700 ГБ свободного дискового пространства.

3. На каждом целевом устройстве установите пакет sudo, если этот пакет еще не установлен. Для операционных систем семейства Debian установите пакет UFW на целевые устройства.

4. На каждом целевом устройстве настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, настройте доступ в интернет, используя прокси-сервер на целевых устройствах.

5. На управляющих узлах с конфигурацией UFW разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

6. Предоставьте доступ к хранилищу пакетов, в котором хранятся следующие пакеты, необходимые для Kaspersky EDR Expert:

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common
   - open-iscsi
   - python3-cffi-backend

- python3-cryptography
- python3-netaddr
- python-apt-common
- systemd
- tar

KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

7. Убедитесь, что установлены следующие пакеты:

   - На каждом целевом устройстве: python3-apt.
   - На управляющих узлах: curl.

   Эти пакеты не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены.

8. Для целевых устройств выключите механизмы защиты от спуфинга ARP/MAC на уровне гипервизора, виртуального коммутатора или сетевой инфраструктуры.

   Для VMware включите **Forged Transmits** и **MAC Address Changes**. Для Hyper-V включите **MAC Address Spoofing**. Для сетевого оборудования выключите **Dynamic ARP Inspection (DAI)** или настройте порт как доверенный.

   В качестве примера см. Руководство по поиску и устранению неисправностей MetalLB, чтобы проверить, достигают ли ARP-запросы узла.

9. Зарезервируйте статические IP-адреса для целевых устройств и шлюзов кластера Kubernetes.

   Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. IP-адрес шлюза является IPv4-адресом (например, 10.80.23.182).

   Для конфигурации в нескольких ЦОД каждый центр обработки данных использует собственный шлюз кластера Kubernetes с выделенным IP-адресом. Он указывается в конфигурационном файле для каждого центра обработки данных (параметр `ingress_ip` в секции `zones`).

   Целевые устройства и шлюз кластера Kubernetes должны находиться в одной подсети одного центра обработки данных.

   > Для шлюза кластера Kubernetes и целевых устройств требуется IPv4-адресация. Если в вашей среде требуется подключение по протоколу IPv6, настройте операционные системы на целевых устройствах и шлюзе кластера Kubernetes для маршрутизации трафика IPv6 через шлюз IPv6 (NAT64) или туннель IPv6. Эта конфигурация поддерживает работу кластера на IPv4, обеспечивая взаимодействие с сетями IPv6.

10. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Kaspersky EDR Expert.

    По умолчанию службы Kaspersky EDR Expert доступны по следующим адресам:

    - <console_host>.<smp_domain>
    - <ksc_host>.<smp_domain>
    - <kuma_host>.<smp_domain>

- <api_host>.<smp_domain>
- <monitoring_host>.<smp_domain>
- <xdr_edr_ingress_host>.<smp_domain>
- <updater>.<smp_domain>

  Где <console_host>, <ksc_host>, <kuma_host>, <api_host>, <monitoring_host>, <xdr_edr_ingress_host> и <updater> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями служб FQDN, которые вы можете указать в конфигурационном файле. Если вы не указываете пользовательские значения имен служб устройств, используются значения по умолчанию: `console_host` – `"console"`, `ksc_host` – `"admsrv"`, `kuma_host` – `"kuma"`, `api_host` – `"api"`, `monitoring_host` – `"monitoring"`, `xdr_edr_ingress_host` – `"agentserver"`, `updater` – `"updater"`.

Перечисленные FQDN служб должны разрешаться в IP-адрес в управляемом заказчиком балансировщике нагрузки.

Например:

- <load_balancer_host_ip> – admsrv.<smp_domain>
- <load_balancer_host_ip> – api.<smp_domain>
- <load_balancer_host_ip> – console.<smp_domain>
- <load_balancer_host_ip> – kuma.<smp_domain>
- <load_balancer_host_ip> – *.kuma.<smp_domain>
- <load_balancer_host_ip> – monitoring.<smp_domain>
- <load_balancer_host_ip> – agentserver.<smp_domain>
- <load_balancer_host_ip> – updater.<smp_domain>

11. На целевых устройствах создайте учетные записи, которые будут использоваться для развертывания Kaspersky EDR Expert.

    Эти учетные записи используются для SSH-соединения и должны иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

    Просмотреть информацию

    Чтобы добавить созданные учетные записи пользователей в файл `/etc/sudoers`:

    1. Выполните следующие команды:

       ```
       sudo useradd -m -s /bin/bash <имя_пользователя>
       sudo usermod -aG sudo <имя_пользователя>
       ```

    2. Откройте файл `/etc/sudoers` с помощью команды:

       ```
       sudo visudo
       ```

3. Добавьте следующую строку в конец секции `# Allow members of group sudo to execute any command`:

   ```
   <имя_пользователя> ALL=(ALL) NOPASSWD: ALL
   ```

   Где `<имя_пользователя>` – имя созданного пользователя.

4. Сохраните и закройте файл `/etc/sudoers`.

12. Настройте SSH-соединение между устройством администратора и целевыми устройствами:

    a. На устройстве администратора сгенерируйте SSH-ключи с помощью утилиты ssh-keygen без парольной фразы.

    b. Скопируйте открытый ключ на каждое целевое устройство и, если используется балансировщик нагрузки, на устройство балансировщика нагрузки (например, в директорию `/home/<user_name>/.ssh`) с помощью утилиты ssh-copy-id.

    Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

13. Для корректной работы компонентов Kaspersky EDR Expert обеспечьте сетевой доступ между целевыми устройствами и при необходимости откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

14. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

15. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Kaspersky EDR Expert.

    Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации, или конечные сертификаты для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Развертывание в нескольких ЦОД: параметры установки

Конфигурационный файл – это файл в формате YAML, содержащий набор параметров установки компонентов Kaspersky EDR Expert.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны перед развертыванием Kaspersky EDR Expert. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения. Значения параметров должны соответствовать описанным ниже правилам. Во время развертывания Kaspersky EDR Expert, KDT проверяет, правильно ли указаны нужные параметры установки. Если необходимые параметры в конфигурационном файле отсутствуют или недействительны, развертывание будет прервано.

Пример конфигурационного файла развертывания Kaspersky EDR Expert в нескольких ЦОД

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Infrastructure regions that contain data centers
```

```
regions:
  # Infrastrusture region 1
  prox1:
    # Name of the infrastructure region.
    description: Proxmox1
  # Infrastructure region 2
  prox2:
    # Name of the infrastructure region.
    description: Proxmox2
  # Infrastructure region 3
  prox3:
    # Name of the infrastructure region.
    description: Proxmox3
# Data centers where the Kubernetes cluster nodes are distributed
zones:
  # Data center 1
  proxmox1:
    # Name of the infrastructure region that the data center belongs to.
    region: prox1
    # Kubernetes cluster gateway IP address of the data center 1.
    ingress_ip: 10.0.0.200
  # Data center 2
  proxmox2:
    # Name of the infrastructure region that the data center belongs to.
    region: prox2
    # Kubernetes cluster gateway IP address of the data center 2.
    ingress_ip: 10.10.20.100
  # Data center 3
  proxmox3:
    # Name of the infrastructure region that the data center belongs to.
    region: prox3
    # Kubernetes cluster gateway IP address of the data center 3.
    ingress_ip: 10.65.20.100
# Nodes on which the Kubernetes cluster and Kaspersky EDR will be deployed
nodes:
  # Data center 1 - primary node
  - desc: cdt-primary1
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
    zone: proxmox1
    # IP address of the node.
    host: 10.0.0.100
    access:
      ssh:
        # User name of the account.
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
        # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
        помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
        key: /root/.ssh/id_rsa
  # Data center 2 - primary node
  - desc: cdt-primary2
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
```

```
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.18
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 3 - primary node
- desc: cdt-primary3
  # Node type.
  type: primary
  # Name of the data center that the node belongs to.
  zone: proxmox3
  # IP address of the node.
  host: 10.65.20.100
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 1
- desc: cdt-w1
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.101
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 2
- desc: cdt-w2
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.102
  access:
```

```
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 3
- desc: cdt-w3
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.103
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 1
- desc: cdt-w4
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.20
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 2
- desc: cdt-w5
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.21
  access:
    ssh:
      # User name of the account.
      user: root
```

```
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 3
- desc: cdt-w6
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.22
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 3 - worker node 1
- desc: cdt-w7
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox3
  # IP address of the node.
  host: 10.65.20.11
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
# Data center 3 - worker node 2
- desc: cdt-w8
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox3
  # IP address of the node.
  host: 10.65.20.12
  access:
    ssh:
      # User name of the account.
      user: root
      # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
      в параметре ssh_pk.
      # password: pass
```

```
      # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
      помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
      key: /root/.ssh/id_rsa
  # Data center 3 - worker node 3
  - desc: cdt-w9
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.13
    access:
      ssh:
        # User name of the account.
        user: root
        # Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного
        в параметре ssh_pk.
        # password: pass
        # Путь к закрытой части SSH-ключа для подключения к первичному рабочему узлу с
        помощью KDT. Закрытая часть SSH-ключа расположена на устройстве администратора.
        key: /root/.ssh/id_rsa
# Parameters for the Kaspersky EDR deployment
parameters:
  # Connection string for accessing the DBMS installed and configured on a separate
  server.
  # user_db – имя пользователя привилегированной внутренней учетной записи СУБД. Этой
  учетной записи предоставлены права на создание баз данных и других учетных записей
  СУБД.
  # password_db – пароль привилегированной внутренней учетной записи СУБД.
  # fqdn_db:port_db—The FQDN and connection port of a separate server on which the DBMS
  is installed.
  # Значение параметра 'psql_dsn' должно соответствовать URI-формату. Если URI-
  подключение включает специальные символы в любой из его частей, символы должны быть
  экранированы с помощью процентной кодировки.
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  # Path to the SSH private key for connection to the primary and workers nodes by KDT.
  Закрытая часть SSH-ключа расположена на устройстве администратора.
  # The parameter value must be a Linux file path or Base64-encoded file content.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky EDR user account that will be created during the
  installation.
  # Password must be 8 to 256 characters long.
  # It can contain lowercase or uppercase letters ('a' to 'z'), digits ('0' to '9'), and
  special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - name: admin_password
    source:
      value: "password"
  # Путь к файлу инвентаря KUMA, который содержит параметры установки для развертывания
  сервисов KUMA. Этот файл расположен на устройстве администратора.
  # Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
  Base64.
  - name: inventory
    source:
      value: "/home/user/inventory.yml"
```

```
# Путь к лицензионному ключу Kaspersky Endpoint Detection and Response. Этот файл
расположен на устройстве администратора.
# Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке
Base64.
- name: license
  source:
    value: "/home/user/license.key"
# Domain name. Значение параметра должно соответствовать требованиям назначения имен
доменов до четвертого уровня.
# The service host name and domain name are parts of FQDNs of the Kaspersky EDR
services.
# Значения по умолчанию для имен служб устройств: nwc_host—"console", flow_host
—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host
—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom host names can be specified in the configuration file.
# Пример: console.smp.local является FQDN службы, предоставляющей доступ к Консоли
OSMP. Этот FQDN состоит из значений параметров 'console_host' и 'smp_domain'.
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky EDR services for which a self-signed or custom
certificate must be generated.
# Значение параметра должно быть списком имен устройств, разделенных пробелами. Если
пользовательские имена устройств не указаны, используются имена устройств по умолчанию:
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring agentserver updater"
# The parameter that indicates whether to deploy the KUMA services for Kaspersky EDR or
for Kaspersky NGFW.
- name: autodeploy_plan
  source:
    value: "edr"
# User name for authentication on the SMTP server.
- name: grafana_admin_user
  source:
    value: xdr
# Password for authentication on the SMTP server.
- name: grafana_admin_password
  source:
    value: "password"
```

Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Секция `regions` содержит параметры установки для каждого региона логической инфраструктуры. Регион представляет собой географическую область или местоположение развертывания и группирует один или несколько центров обработки данных (зон).

Секция regions

Имя параметра	Обязательная	Описание

`description`	Да	Название региона инфраструктуры.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Все регионы инфраструктуры должны иметь уникальные имена.

Секция `zones` содержит параметры установки для каждого центра обработки данных. Каждая зона принадлежит определенному региону.

Секция zones

Имя параметра	Обязательная	Описание

`region`	Да	Название региона инфраструктуры, к которому принадлежит зона.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Значение параметра `region` должно соответствовать идентификатору региона, заданному в секции `regions`.

`ingress_ip`	Да	Зарезервированный статический IPv4-адрес шлюза кластера Kubernetes. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. У каждого центра обработки данных должен быть свой уникальный IP-адрес шлюза кластера. Шлюз должен быть включен в ту же подсеть, что и управляющие рабочие узлы кластера, расположенные в одном центре обработки данных.

Раздел `nodes` конфигурационного файла содержит параметры установки для каждого целевого устройства кластера Kubernetes. Эти параметры перечислены в таблице ниже.

Раздел nodes

Имя параметра	Обязательная	Описание

`desc`	Да	Имя узла.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Все узлы кластера должны иметь уникальные имена. Это требование является одним из обязательных для установки Kaspersky EDR Expert и проверяется с помощью KDT.

`type`	Да	Тип узла. Возможные значения параметра: • `primary` • `worker`

Имя параметра	Обязательная	Описание
`host`	Да	IP-адрес узла. Все узлы, принадлежащие центру обработки данных, должны быть включены в ту же подсеть, что и шлюз кластера Kubernetes этого центра обработки данных. Для узлов требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера.
`zone`	Да	Название центра обработки данных, к которому принадлежит узел. Значение параметра `zone` должно соответствовать центру обработки данных, заданному в секции `zones`.
`kuma_role`	Нет	Служба KUMA, которую вы можете указать для установки на рабочем узле. Можете задать установку одного или нескольких служб KUMA, либо не указывать их установку. Параметр `kuma_roles` учитывается при установке службы KUMA в кластере Kubernetes с помощью Консоли OSMP. Если узел, на котором вы планируете установить службу KUMA, перегружен, кластер выберет другой, менее загруженный узел для установки службы. Для параметра `inventory` установите значение `/dev/null`. Хранилища, созданные из одного ресурса KUMA, не разрешается размещать на одном рабочем узле. Данное правило добавлено для обеспечения необходимого уровня отказоустойчивости. Возможные значения параметра: • `core` – ядро KUMA • `metrics` – просмотр метрик KUMA • `collector` – коллектор • `correlator` – коррелятор • `storage` – хранилище Значение параметра указывается в виде списка строк, включающих в себя роли KUMA. Например: `kuma_roles: ["core","metrics","collector"]`

`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 31 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • нижнее подчеркивание (_), дефис (-).

`password`	Нет	Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного в параметре `ssh_pk`.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Имя параметра	Обязательная	Описание
psql_dsn	Да	Строка подключения для доступа к СУБД, которая установлена и настроена вне кластера Kubernetes. Укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port> где: • dbms_username – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Kaspersky EDR Expert. • password – пароль привилегированной внутренней учетной записи СУБД. • fqdn:port – полное имя домена и порт подключения целевого устройства, на котором установлена СУБД. Чтобы использовать кластер высокой доступности, укажите этот параметр следующим образом: psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port> Чтобы использовать Corosync/Pacemaker, укажите этот параметр с виртуальным IP-адресом следующим образом: psql_dsn=postgres://postgres:pass!@<virtual ip>:<port> Значение параметра psql_dsn должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки. Символы, которые требуется заменить в значении параметра psql_dsn: • Пробел → %20 • ! → %21 • # → %23 • % → %25 • & → %26 • / → %2F • : → %3A • = → %3D • ? → %3F • @ → %40 • [→ %5B •] → %5D Дополнительную информацию см. в статье Строка подключения PostgreSQL.
nwc-language	Да	Язык интерфейса OSMP Console, указанный по умолчанию. После установки вы можете изменить язык OSMP Console. Возможные значения параметра: • enUS (значение по умолчанию) • ruRu Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
ssh_pk	Да	Путь к закрытой части SSH-ключа, которая находится на устройстве администратора и используется для подключения к управляющему рабочему узлу и к узлам со службами KUMA (коллекторам, корреляторам и хранилищам) с помощью утилиты KDT. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.

Имя параметра	Обязательная	Описание
`admin_password`	Да	Параметр `admin_password` задает пароль Kaspersky EDR Expert, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 10 или более 256 символов. • Пароль должен содержать символы как минимум трех групп из списка ниже: • верхний регистр (A–Z); • нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;). • Пароль не должен содержать пробелов или комбинации ".@". Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера развертывания), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Нет	Параметр, указывающий на то, что приложение Kaspersky EDR Expert установлено на целевом устройстве с ограниченными вычислительными ресурсами. В случае развертывания на нескольких узлах установите для параметра `low_resources` значение `false`. Возможные значения параметра: • `true` – установка с ограниченными вычислительными ресурсами (для развертывания на одном узле). • `false` – стандартная установка (значение по умолчанию).
`core_disk_request`	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `false` или ничего не указано, для работы Ядра KUMA будет выделен объем дискового пространства 100 ГБ по умолчанию. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `true`, для работы Ядра KUMA будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр `core_disk_request` позже, после развертывания приложения.
`metrics_disk_request`	Да	Параметр, задающий объем дискового пространства для работы службы Метрики. Если параметр `metrics_disk_request` не задан, а для параметра `low_resources` установлено значение `false` или не установлено значение, для работы службы Метрики будет выделен объем дискового пространства 80 ГБ по умолчанию. Если параметр `metrics_disk_request` не задан, а для параметра `low_resources` установлено значение `true`, для работы службы Метрики будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр `metrics_disk_request` позже, после развертывания приложения.
`inventory`	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если все сервисы KUMA будут установлены внутри кластера, для параметра `inventory` установите значение `/dev/null`.

Имя параметра	Обязательная	Описание
`host_inventory`	Нет	Путь к дополнительному файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если вы выполняете первоначальное развертывание Kaspersky EDR Expert или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (`/dev/null`).
`license`	Нет	Путь к KUMA лицензионному ключу, находящемуся на устройстве администратора. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Вы можете загрузить лицензионный ключ или указать код активации при входе в OSMP после завершения развертывания.

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
`xdr_edr_ingress_host`
	Да	Имя устройства, которое используется в FQDN публичных служб Kaspersky EDR Expert. Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.
		Если пользовательские имена устройств не указаны, используются следующие имена устройств по умолчанию:
		• `nwc_host – "console"`
		• `flow_host – "console"`
		• `hydra_host – "console"`
		• `login_host – "console"`
		• `ksc_host–"admsrv"`
		• `console_host – "console"`
		• `api_host – "api"`
		• `kuma_host – "kuma"`
		• `monitoring_host – "monitoring"`
		• `xdr_edr_ingress_host–"agentserver"`

`smp_domain`	Да	Имя домена, которое используется в FQDN публичных служб Kaspersky EDR Expert. Значение параметра должно соответствовать требованиям назначения имен доменов до четвертого уровня. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.
`pki_host_list`	Да	Список имен устройств публичных служб Kaspersky EDR Expert, для которых требуется сформировать самоподписанный или пользовательский сертификат. Значение параметра должно быть списком имен устройств разделенных пробелами.
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Kaspersky EDR Expert. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат. • `false` – использовать самоподписанные сертификаты (значение по умолчанию).
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, который используется для работы с общедоступными службами Kaspersky EDR Expert. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.

Имя параметра	Обязательная	Описание

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с соответствующими публичными службами Kaspersky EDR Expert: `<admsrv_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<kuma_host>.<smp_domain>`, `<monitoring_host>.<smp_domain>` и `<console_host>.<smp_domain>`. Значения параметров должны быть Linux-путем к файлу или содержимым файла в кодировке Base64.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметры `intermediate_bundle` и `pki_host_list`.

`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных). Измеряется в гигабайтах, указывается как "<объем>Gi". Требуемый объем свободного места на диске зависит от количества управляемых устройств и других параметров и может быть рассчитан. Значение по умолчанию – 30 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Измеряется в гигабайтах, указывается как "<объем>GB". Минимальное рекомендуемое значение и значение по умолчанию – 5 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.

`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 30 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (_ - .)
		• Имя пользователя должно начинаться с буквы.
		• Имя пользователя не должно содержать пробелов или символа "@".

`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Пароль должен соответствовать следующим правилам:
		• Пароль пользователя не может содержать менее 8 или более 256 символов.
		• Пароль должен содержать символы из указанных ниже групп:
		  • верхний регистр (A–Z);
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Измеряется в гигабайтах, указывается как " <объем>Gi". Минимальное рекомендуемое значение и значение по умолчанию – 40 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. По умолчанию указано значение 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h"). Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.

Имя параметра	Обязательная	Описание
psql_tls_off	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Kaspersky EDR Expert и СУБД по протоколу TLS. Если СУБД установлена за пределами кластера, шифрование TLS выключено по умолчанию (значение по умолчанию true). Возможные значения параметра: • true – трафик не шифруется (значение по умолчанию). • false – трафик шифруется.
psql_trusted_cas	Нет	Путь к PEM-файлу, который может содержать TLS-сертификат сервера СУБД или корневой сертификат, из которого может быть выдан сертификат TLS-сервера. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Укажите параметр psql_trusted_cas, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра psql_tls_off указано значение false).
proxy_enabled	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Kaspersky EDR Expert к интернету. Если устройство, на котором установлен Kaspersky EDR Expert, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Kaspersky EDR Expert (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. Возможные значения параметра: • true – использовать прокси-сервер. • false – не использовать прокси-сервер (значение по умолчанию).
proxy_addresses	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "0.0.0.0 0.0.0.1 0.0.0.2"). Укажите этот параметр, если для параметра proxy_enabled указано значение true.
proxy_port	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра proxy_enabled указано значение true.
trace_level	Нет	Уровень детализации файлов трассировки Сервера администрирования. Трассировка записывается во время работы Сервера администрирования. Значение по умолчанию – 0, трассировка не записывается. Возможные значения параметра: 0–5. Чем выше значение параметра, тем более подробная информация о трассировке записывается.
ansible_extra_flags	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • -v • -vv • -vvv • -vvvv По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.
incident_attachments_max_count_limit	Нет	Количество файлов, которые вы можете прикрепить к инциденту. По умолчанию указано значение 100.
incident_attachments_max_size_limit	Нет	Общий размер файлов, прикрепленных к инциденту. Измеряется в байтах. Единицы измерения не отображаются. По умолчанию указано значение 26214400.

Имя параметра	Обязательная	Описание
`ignore_precheck`	Нет	Параметр, указывающий, следует ли проверить аппаратное и программное обеспечение, а также конфигурацию сети узлов кластера Kubernetes на соответствие требованиям, необходимым для установки решения перед развертыванием. Возможные значения параметра: • `true` – пропустить предварительные проверки. • `false` – выполнить предварительные проверки (значение по умолчанию).
`airgap_mode`	Нет	Параметр, включающий или выключающий предварительную проверку и обновление кеша пакетов пакетным менеджером APT. Таким образом становится возможным развертывание Kaspersky EDR Expert в среде с физической изоляцией. Возможные значения параметра: • `true` – пропустить предварительную проверку и обновление кеша пакетов. • `false` – выполнить предварительную проверку и обновление кеша пакетов (значение по умолчанию).
`grafana_smtp_host`	Нет	Адрес SMTP-сервера для Grafana, который используется для отправки уведомлений о событиях, связанных с работоспособностью кластера Kubernetes, по электронной почте. Укажите этот параметр в формате `<хост>:<порт>` – например, `localhost:25`.
`grafana_smtp_user`	Нет	Имя пользователя для аутентификации на SMTP-сервере.
`grafana_smtp_password`	Нет	Пароль для аутентификации на SMTP-сервере.
`grafana_smtp_bundle`	Нет	Файл, содержащий цепочку сертификатов X.509, которая используется для проверки TLS-подключения к SMTP-серверу.
`grafana_smtp_skip_verify`	Нет	Данный параметр указывает, следует ли пропускать проверку TLS-сертификата для SMTP-сервера. Возможные значения параметра: • `true` – пропустить проверку TLS-сертификата. • `false` – выполнять проверку TLS-сертификата (значение по умолчанию).
`grafana_smtp_from_address`	Нет	Электронный адрес отправителя, который будет отображаться в поле "От" при отправке уведомлений по электронной почте.
`grafana_smtp_from_name`	Нет	Отображаемое имя отправителя в уведомлениях по электронной почте.
`grafana_smtp_ehlo_identity`	Нет	Идентификатор, используемый в команде EHLO при подключении к SMTP-серверу.
`grafana_starttls_policy`	Нет	Политика использования STARTTLS при подключении к SMTP-серверу. Возможные значения параметра: • `OpportunisticStartTLS` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования. • `MandatoryStartTLS` – требовать STARTTLS и завершаться с ошибкой, если SMTP-сервер не поддерживает STARTTLS. • `NoStartTLS` – не использовать STARTTLS и подключиться к SMPT-серверу без шифрования. • `empty` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования (значение по умолчанию).
`grafana_smtp_enable_tracing`	Нет	Параметр, который указывает, следует ли включить ли трассировку SMTP-подключения для отладки отправки электронной почты. Возможные значения параметра: • `true` – включить трассировку SMTP-подключения. • `false` – отключить трассировку SMTP-подключения (значение по умолчанию).

Имя параметра	Обязательная	Описание
autodeploy_plan	Нет	Параметр, указывающий, следует ли развертывать сервисы KUMA для Kaspersky EDR или для Kaspersky NGFW. Возможные значения параметра: • edr – развернуть службы KUMA для OSMP и Kaspersky EDR в кластере Kubernetes (значение по умолчанию). • ngfw – развернуть службы KUMA для OSMP и Kaspersky NGFW внутри кластера Kubernetes. Также предустановленный коллектор **[OOTB] Kaspersky NGFW** будет установлен на первом устройстве из списка устройств, указанного в параметре kuma_collector файла инвентаря KUMA. • none – не разворачивать службы KUMA для Kaspersky EDR или Kaspersky NGFW. Это значение следует указывать при развертывании Kaspersky EDR Expert без сервисов KUMA для Kaspersky EDR и Kaspersky NGFW или при восстановлении Kaspersky EDR Expert из резервной копии. Если при восстановлении Kaspersky EDR Expert задать значения edr или ngfw, это может привести к конфликту между развернутыми сервисами и сервисами из резервной копии.
tokenhub_access_token	Нет	Время жизни токена доступа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "1h10m" или "2h". Минимальное значение – 5m, а максимальное значение – 2h. Значение по умолчанию – 1h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр tokenhub_access_token позже, после развертывания приложения.
tokenhub_refresh_token	Нет	Время жизни токена обновления, используемого для получения нового токена доступа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1240h30m". Минимальное значение – 12m, а максимальное значение – 4320h. Значение по умолчанию – 24h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр tokenhub_refresh_token позже, после развертывания приложения.
credentials_session_ttl	Нет	Максимальное время простоя сеанса единого входа. В конфигурационном файле установите значение параметра – "<time in hours>h<time in minutes>m<time in seconds>s". Например, "24h" или "1h30m". Минимальное значение – 5m, а максимальное значение – 96h. Значение по умолчанию – 1h. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр credentials_session_ttl позже, после развертывания приложения.

Развертывание в нескольких ЦОД с перекрестным подключением с помощью стандартной виртуальной машины Ubuntu Server 24.04 LTS

В этом разделе содержатся инструкции по развертыванию Kaspersky EDR Expert в нескольких ЦОД с перекрестным подключением в нескольких центрах обработки данных на стандартной виртуальной машине Ubuntu Server 24.04 LTS.

1 Типовая конфигурация из трех основных узлов, девяти рабочих узлов и HAProxy

В этом развертывании используется три центра обработки данных, по одному основному узлу и тремя рабочими узлами в каждом. Всего для этого развертывания требуется три основных узла, девять рабочих узлов и один узел HAProxy. Требования к узлам:

- Управляющий узел: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 500 ГБ
- Рабочий узел: 10 vCPU, 20 ГБ оперативной памяти, SSD* объемом 1 ТБ
- Узел HAProxy: 4 vCPU, 8 ГБ оперативной памяти, SSD* объемом 100 ГБ

* Или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

> Требования к оборудованию должны быть рассчитаны в соответствии с руководством по масштабированию.

2 Настройка HAProxy и управляющего и рабочего узлов

2.1 Настройка устройства HAProxy

Для реализации решения с использованием нескольких ЦОД хосты должны быть распределены по разным подсетям с использованием трех шлюзов кластера Kubernetes из них, а узел HAProxy должен быть расположен в одной из подсетей.

1. Установите HAProxy:

```
sudo apt update
sudo apt install haproxy
```

2. Измените конфигурационный файл HAProxy:

```
sudo nano /etc/haproxy/haproxy.cfg
```

Пример конфигурационного файла:

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
        daemon

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http

listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST

frontend http
  mode tcp
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <IP-адрес первого шлюза>:80 check inter 5s # ingress_ip number 1
  server proxmox2 <IP-адрес второго шлюза>:80 check inter 5s # ingress_ip number 2
  server proxmox3 <IP-адрес третьего шлюза>:80 check inter 5s # ingress_ip number 3

frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <IP-адрес первого шлюза>:443 check inter 5s # ingress_ip number 1
  server proxmox2 <IP-адрес второго шлюза>:443 check inter 5s # ingress_ip number 2
  server proxmox3 <IP-адрес третьего шлюза>:443 check inter 5s # ingress_ip number 3

frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
```

```
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <IP-адрес первого шлюза>:9443 check inter 5s  # ingress_ip number 1
  server proxmox2 <IP-адрес второго шлюза>:9443 check inter 5s  # ingress_ip number 2
  server proxmox3 <IP-адрес третьего шлюза>:9443 check inter 5s # ingress_ip number 3

frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <IP-адрес первого шлюза>:4443 check inter 5s # ingress_ip number 1
  server proxmox2 <IP-адрес второго шлюза>:4443 check inter 5s # ingress_ip number 2
  server proxmox3 <IP-адрес третьего шлюза>:4443 check inter 5s # ingress_ip number 3

frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <IP-адрес первого шлюза>:13000 check inter 5s # ingress_ip number 1
  server proxmox2 <IP-адрес второго шлюза>:13000 check inter 5s # ingress_ip number 2
  server proxmox3 <IP-адрес третьего шлюза>:13000 check inter 5s # ingress_ip number 3
```

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

4. Перезапустите службу HAProxy:

```
sudo systemctl restart haproxy
```

2.2 Настройка управляющего и рабочего узлов

2.2.1 Настройка учетной записи пользователя для развертывания Kaspersky EDR Expert

1. Откройте /etc/sudoers:

```
sudo visudo
```

2. Добавьте в конец файла следующую строку:

```
{user} ALL=(ALL) NOPASSWD: ALL
```

где `{user}` – учетная запись, используемая для развертывания.

3. Сохраните (**`Ctrl+S`**) и закройте файл (**`Ctrl+X`**).

2.2.2 Проверка свободного места в директориях /var, /opt и /tmp

1. На управляющем узле выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2. На узлах worker1–worker3 выполните следующие команды:

   ```
   df -h /var
   ```

   Требуется не менее 200 ГБ свободного места.

   ```
   df -h /opt
   ```

   Требуется не менее 700 ГБ свободного места.

   ```
   df -h /tmp
   ```

   Требуется не менее 50 ГБ свободного места.

2.2.3 Обеспечение отсутствия ошибок при синхронизации репозиториев

Выполните следующую команду:

```
sudo apt update
```

Команда не должна возвращать ошибки.

2.2.3 Установка python3-apt и curl

Выполните следующую команду:

```
sudo apt install python3-apt curl -y
```

2.2.4 Настройка системного времени для синхронизации с NTP-сервером

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

3 Настройка устройства СУБД

Устройство СУБД – это устройство с установленным экземпляром СУБД.

Требования к устройству, на котором установлен экземпляр СУБД:

- 10 vCPU
- 20 ГБ оперативной памяти
- 1.6 ТБ SSD или любое устройство с 8000 IOPS (операций ввода-вывода в секунду) при произвольном доступе

Поддерживаемые версии PostgreSQL см. в статье Аппаратные и программные требования.

3.1 Установка и настройка PostgreSQL

1. Установите PostgreSQL:

```
sudo apt install -y postgresql-<версия>
```

   где `<версия>` – поддерживаемые версии PostgreSQL.

   Если требуемая версия PostgreSQL отсутствует в подключенном репозитории, необходимо добавить репозиторий `postgresql`. Подробнее см. на сайте PostgreSQL.

2. Создайте отдельного суперпользователя PostgreSQL:

```
sudo -u postgres createuser --superuser xdr
```

3. Укажите пароль пользователя:

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
```

4. Создайте для пользователя базу данных с таким же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<версия>/main/pg_hba.conf
```

где `<версия>` – поддерживаемые версии PostgreSQL.

6. Укажите следующие параметры в конфигурационном файле PostgreSQL (/etc/postgresql/`<версия>`/main/postgresql.conf), где `<версия>` – версия PostgreSQL. Например, для PostgreSQL 16: /etc/postgresql/16/main/postgresql.conf.

   Прокомментированные (#) строки необходимо раскомментировать.

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4 Настройка устройства администратора

Устройство администратора – это устройство, с которого запускается утилита KDT. Файлы из дистрибутива, включая архив с утилитой KDT, должны находиться на хосте администратора. Это устройство может быть частью кластера Kubernetes, созданного утилитой KDT во время развертывания, или может оставаться за пределами кластера. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и OSMP. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов OSMP.

4.1 Распаковка утилиты KDT

Выполните следующую команду, чтобы создать директорию и распаковать утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Установка Docker

Поддерживаются версии Docker 25 и выше.

4.2.1 Установка в Ubuntu 24:

```
sudo apt update && sudo apt install docker.io
```

4.2.2 **ИЛИ** *Установка с использованием официальной инструкции:*

1. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

2. Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
/etc/apt/keyrings/docker.asc
```

3. Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

4. Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
plugin
```

4.3 Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Активируйте членство пользователя в группе `docker` в текущем сеансе:

```
newgrp docker
```

4.4 Настройка системного времени для синхронизации с NTP-сервером:

1. Выполните следующие команды:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

   В выводе будет строка:

```
System clock synchronized: yes
```

2. Чтобы проверить синхронизацию, выполните команду:

```
date
```

   В выводе будет текущая дата и время.

4.5 Проверка свободного места в директории /tmp

Выполните следующую команду:

```
df -h /tmp
```

Требуется не менее 50 ГБ свободного места.

Если у вас недостаточно свободного места в директории /tmp, укажите путь к другой директории:

```
export TMPDIR=<новая_директория>/tmp
```

Или добавьте место в необходимом объеме:

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

Выделив необходимое место, перезагрузите хост или повторно смонтируйте раздел.

4.6 Настройка SSH-соединения между устройством администратора и основными и рабочими узлами

1. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. Скопируйте ключ на каждый целевой хост по очереди:

```
ssh-copy-id {user}@{primary_ip}
ssh-copy-id {user}@{worker_ip}  # копирование ключа для каждого рабочего узла в подсети
```

Где `{user}` – учетная запись пользователя для развертывания Kaspersky EDR Expert, созданная во время настройки целевого устройства.

4.7 Настройка DNS

На вашем DNS-сервере зарегистрируйте FQDN служб для подключения к службам OSMP (`<smp_domain>`).

Чтобы быстро начать работу, добавьте на свой DNS-сервер запись подстановки A, указывающую на IP-адрес HAProxy. HAProxy балансирует трафик между тремя шлюзами кластера Kubernetes (`<ingress_ip>`), которые затем направляют трафик в соответствующие службы.

По умолчанию службы OSMP доступны по следующим адресам:

```
<haproxy_host_ip> - admsrv.<smp_domain>
<haproxy_host_ip> - api.<smp_domain>
<haproxy_host_ip> - console.<smp_domain>
<haproxy_host_ip> - kuma.<smp_domain>
<haproxy_host_ip> - *.kuma.<smp_domain>
<haproxy_host_ip> - monitoring.<smp_domain>
<haproxy_host_ip> - agentserver.<smp_domain>
<haproxy_host_ip> - updater.<smp_domain>
```

4.8 Создание конфигурации для запуска установки

Легенда

- `10.0.0.100` – IP-адрес первого основного узла первой подсети (`<primary1_ip>`)
- `10.10.20.18` – IP-адрес второго основного узла второй подсети (`<primary2_ip>`)
- `10.65.20.10` – IP-адрес третьего основного узла третьей подсети (`<primary3_ip>`)
- `10.0.0.101` – IP-адрес первого рабочего узла первой подсети (`<worker1_ip>`)
- `10.0.0.102` – IP-адрес второго рабочего узла первой подсети (`<worker2_ip>`)
- `10.0.0.103` – IP-адрес третьего рабочего узла первой подсети (`<worker3_ip>`)
- `10.10.20.20` – IP-адрес первого рабочего узла второй подсети (`<worker4_ip>`)
- `10.10.20.21` – IP-адрес второго рабочего узла второй подсети (`<worker5_ip>`)
- `10.10.20.22` – IP-адрес третьего рабочего узла второй подсети (`<worker6ip>`)

- `10.65.20.11` – IP-адрес первого рабочего узла третьей подсети (`<worker7_ip>`)
- `10.65.20.12` – IP-адрес второго рабочего узла третьей подсети (`<worker8_ip>`)
- `10.65.20.13` – IP-адрес третьего рабочего узла третьей подсети (`<worker9_ip>`)
- `10.0.0.150` – IP-адрес устройства СУБД (`<DB_ip>`)
- `10.0.0.200` – IP-адрес первого шлюза кластера Kubernetes
- `10.10.20.100` – IP-адрес второго шлюза кластера Kubernetes
- `10.65.20.100` – IP-адрес третьего шлюза кластера Kubernetes
- `10.0.0.111` – IP-адрес устройства HAProxy
- `user` – учетная запись пользователя для развертывания (`<user_name>`)
- `/home/user/.ssh/id_rsa` – путь к SSH-ключу, созданному при настройке SSH-соединения на устройстве администратора (`<ssh_key_path>`)
- `xdr.mydomain.com` – домен для входящего трафика (`<smp_domain>`)

4.8.1 Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT.

Значение параметра `psql_dsn` должно соответствовать URI-формату. Если URI-подключение включает специальные символы в любой из его частей, символы должны быть экранированы с помощью процентной кодировки.

Символы, которые требуется заменить в значении параметра `psql_dsn`:

- Пробел → `%20`
- `!` → `%21`
- `#` → `%23`
- `%` → `%25`
- `&` → `%26`
- `/` → `%2F`
- `:` → `%3A`
- `=` → `%3D`
- `?` → `%3F`
- `@` → `%40`
- `[` → `%5B`
- `]` → `%5D`

Дополнительную информацию см. в статье Строка подключения PostgreSQL.

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
regions:
    prox1:
        description: Proxmox1
    prox2:
        description: Proxmox2
    prox3:
        description: Proxmox3
zones:
```

```yaml
    proxmox1:
        region: prox1
        ingress_ip: 10.0.0.200
    proxmox2:
        region: prox2
        ingress_ip: 10.10.20.100
    proxmox3:
        region: prox3
        ingress_ip: 10.65.20.100
nodes:
  - desc: cdt-primary1
    type: primary
    zone: proxmox1
    host: 10.0.0.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary2
    type: primary
    zone: proxmox2
    host: 10.10.20.18
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary3
    type: primary
    zone: proxmox3
    host: 10.65.20.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    zone: proxmox1
    host: 10.0.0.101
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    zone: proxmox1
    host: 10.0.0.102
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w3
    type: worker
    zone: proxmox1
    host: 10.0.0.103
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w4
    type: worker
    zone: proxmox2
    host: 10.10.20.20
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w5
    type: worker
    zone: proxmox2
    host: 10.10.20.21
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w6
    type: worker
    zone: proxmox2
    host: 10.10.20.22
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
```

```
  - desc: cdt-w7
    type: worker
    zone: proxmox3
    host: 10.65.20.11
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w8
    type: worker
    zone: proxmox3
    host: 10.65.20.12
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w9
    type: worker
    zone: proxmox3
    host: 10.65.20.13
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<ваш_пароль>@<DB_ip>:5432
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "your_password"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<домен_smp>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "your_password"
```

5 Установка Kaspersky EDR Expert

Выполните следующую команду:

```
./kdt/bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

Если установка завершится успешно, в терминале будет отображена следующая информация:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
```

```
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, требуется перейти на страницу авторизации. Для этого введите в строке поиска браузера:

```
console.<smp_domain>
```

Где `<smp_domain>` – FQDN, указанное на шаге 4.7 этой процедуры.

Обслуживание Kaspersky EDR Expert

В этом разделе описано обновление, удаление и переустановка компонентов Kaspersky EDR Expert с помощью KDT. Также в разделе приведены инструкции по остановке узлов кластера Kubernetes, обновлению пользовательских сертификатов для публичных служб Kaspersky EDR Expert, получению текущей версии конфигурационного файла и выполнению других действий с компонентами Kaspersky EDR Expert с помощью KDT.

Обновление компонентов Kaspersky EDR Expert

KDT позволяет обновлять компоненты Kaspersky EDR Expert (включая веб-плагины управления) и компонент Bootstrap. В дистрибутив включены новые версии компонентов Kaspersky EDR Expert.

Установка компонентов более ранней версии не поддерживается.

Чтобы обновить компоненты Kaspersky EDR Expert:

1. Загрузите дистрибутив с новыми версиями компонентов Kaspersky EDR Expert.

2. При необходимости экспортируйте текущую версию конфигурационного файла на устройстве администратора.

   Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.

3. Обновите компоненты Kaspersky EDR Expert Bootstrap.

   Укажите путь к транспортному архиву с компонентами Kaspersky EDR Expert и путь к конфигурационному файлу. Путь к конфигурационному файлу не является обязательным, если он указан в команде обновления Bootstrap или параметры установки не добавлены или не изменены:

   - Выполните команду для стандартного обновления компонентов Kaspersky EDR Expert:

     ```
     ./kdt apply -k <полный_путь_к_архиву_обновлений_XDR> -i
     <полный_путь_к_конфигурационному_файлу>
     ```

- Если версия установленного компонента Kaspersky EDR Expert совпадает с версией компонента в дистрибутиве, обновление этого компонента пропускается. Выполните команду, чтобы принудительно обновить этот компонент с помощью флага `force`:

  ```
  ./kdt apply --force -k <полный_путь_к_архиву_обновлений_XDR> -i
  <полный_путь_к_конфигурационному_файлу>
  ```

4. Если появится новая версия Лицензионного соглашения и Политики конфиденциальности, прочтите Лицензионное соглашение и Политику конфиденциальности компонента Kaspersky EDR Expert. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

      Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать компонент Kaspersky EDR Expert, вам нужно принять условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны) в соответствии с Политикой конфиденциальности.

      Введите `n`, если вы не принимаете условия Политики конфиденциальности.

   Чтобы обновить компонент Kaspersky EDR Expert, вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности.

После того как вы примете Лицензионное соглашение и Политику конфиденциальности, KDT обновит компоненты Kaspersky EDR Expert.

Вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности компонента Kaspersky EDR Expert после обновления. Файлы находятся в директории `~/kaspersky_eula` пользователя, который запускает установку Kaspersky EDR Expert.

Проверка целостности установленных компонентов Kaspersky EDR Expert

После развертывания Kaspersky EDR Expert вы можете проверить подлинность и целостность компонентов решения. Каждый компонент (CNAB) в транспортном архиве включает в себя файл манифеста в формате XML. Манифест содержит контрольные суммы компонентов и подписан цифровой подписью с использованием 256-битного алгоритма ГОСТ Р 34.11-2012. Эта цифровая подпись позволяет обеспечить достоверность контрольных сумм файлов компонентов и убедиться, что контрольные суммы в манифесте не были изменены.

Вы можете удостовериться, что контрольные суммы компонентов соответствуют контрольным суммам, указанным в манифестах. Это позволяет подтвердить, что компоненты не были изменены и были получены из доверенного источника.

Проверка целостности компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes

Чтобы проверить целостность установленных компонентов Kaspersky EDR Expert:

1. Выполните следующую команду, чтобы извлечь компоненты Kaspersky EDR Expert и их манифесты из развернутого решения в указанную директорию. Из решения извлекаются только компоненты, которые находятся в транспортном архиве:

   ```
   ./kdt extract --reference <путь к транспортному архиву> -d <путь к извлеченным пакетам CNABs>
   ```

   где:

   - `<путь к транспортному архиву>` – путь к транспортному архиву.
   - `<путь к извлеченным пакетам CNABs>` – путь к директории, в которую будут извлечены компоненты решения и их манифесты.

2. Выполните следующую команду из директории с извлеченными компонентами и их манифестами. Утилита `integration_checker` сравнивает контрольные суммы компонентов, извлеченных из развернутого решения, с их контрольными суммами в манифестах, извлеченных из транспортного архива:

   ```
   find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
   signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
   ```

   Пример вывода команды после успешной проверки целостности

   Число манифестов, успешно прошедших проверку, отображается в строке `Manifests` в столбце `succeeded`.

   ```
   ==============================================>
   Summary( failed / skipped / succeeded ):
           Manifests: 0 / 0 / 38
           Files: 0 / 0 / 38
           Directories: 0 / 0 / 0
           Registries: 0 / 0 / 0
           Registry values: 0 / 0 / 0
   ==============================================>
   SUCCEEDED
   ```

   Пример вывода команды после неудачной проверки целостности

   В этом примере манифест был изменен после подписания или возникла проблема с подписью. Число пропущенных манифестов или манифестов, проверка которых не прошла, отображается в строке `Manifests` в столбце `failed`.

   ```
   ==============================================>
   Summary( failed / skipped / succeeded ):
           Manifests: 2 / 0 / 36
           Files: 0 / 0 / 0
           Directories: 0 / 0 / 0
           Registries: 0 / 0 / 0
           Registry values: 0 / 0 / 0
   ==============================================>
   FAILED
   ERR Can't verify digital signature of file "/home/xdr_user/integrity_check.xml". Flags: None: 0x80000106
   (Object is untrusted)
   ```

```
Manifest /home/xdr_user/integrity_check.xml failed. Reason: Can't verify digital signature of file
"/home/xdr_user/integrity_check.xml". Flags: None: 0x80000106 (Object is untrusted)
```

Проверка целостности компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes, выполнена. Если внутри кластера также установлены сервисы KUMA, то их целостность также проверяется.

Вы можете проверить целостность сервисов KUMA, установленных вне кластера Kubernetes.

Изменение параметров Kaspersky EDR Expert без переустановки

Если инфраструктура организации изменилась, может потребоваться быстро изменить основные значения параметров Kaspersky EDR Expert, без переустановки решения. Kaspersky EDR Expert поддерживает изменение IP-адреса кластера Kubernetes (параметр `ingress_ip`) и FQDN сервисов (в частности, изменение доменного имени сервиса, параметр `smp_domain`) с использованием KDT.

Чтобы изменить значения параметров без переустановки Kaspersky EDR Expert:

1. На устройстве администратора выполните экспорт текущей версии конфигурационного файла.
2. В экспортированном конфигурационном файле измените значения параметров `smp_domain` или `ingress_ip`. Вы можете изменить оба параметра или любой параметр по отдельности.

   Если вы разворачиваете Kaspersky EDR Expert в нескольких центрах обработки данных, измените значения параметра `ingress_ip` в конфигурационном файле в секции `zones`.
3. Примените изменения параметров с помощью команды:

   ```
   ./kdt apply -i '<полный_путь_к_обновленному_конфигурационному_файлу>'
   ```

   Значения параметров "`smp_domain`" и "`ingress_ip`" изменены. Kaspersky EDR Expert использует новые значения параметров.

Когда значение параметра `smp_domain` меняется, названия служб FQDN также меняются. Следовательно, KDT перевыпускает все сертификаты необходимые для работы с публичными службами Kaspersky EDR Expert.

Добавление и удаление управляющих и рабочих узлов кластера Kubernetes

Если вам нужно масштабировать кластер Kubernetes для текущей рабочей нагрузки, повысить его отказоустойчивость или оптимизировать вычислительные ресурсы, с помощью KDT вы можете добавлять или удалять управляющие и рабочие узлы, включенные в кластер.

Вы можете добавлять или удалять управляющие и рабочие узлы только в том случае, если приложение Kaspersky EDR Expert развернуто на нескольких узлах.

Добавление новых управляющих и рабочих узлов в кластер Kubernetes

Чтобы добавить новые управляющие и рабочие узлы:

1. Подготовьте целевые устройства, которые будут выполнять роль управляющих и рабочих узлов.

2. На устройстве администратора экспортируйте текущий конфигурационный файл с помощью следующей команды:

   ```
   ./kdt ec -e '<имя_конфигурационного_файла_и_путь>'
   ```

   Текущая версия конфигурационного файла сохраняется в указанной директории с указанным именем.

3. В разделе `nodes` экспортированного конфигурационного файла добавьте параметры одного или нескольких новых узлов (`desc`, `type`, `host`, `kind`, `user` и `key`) и сохраните конфигурационный файл.

4. Скопируйте открытый ключ на каждый новый узел (например, в директорию `~/.ssh`) с помощью утилиты ssh-copy-id.

5. На устройстве администратора выполните следующую команду, чтобы применить измененный конфигурационный файл к кластеру Kubernetes. В команде укажите полный путь к этому конфигурационному файлу:

   ```
   ./kdt apply -i '< полный_путь_к_конфигурационному_файлу >'
   ```

   После запуска команды, KDT проверяет правильность заполнения конфигурационного файла. Далее KDT проверяет, соответствует ли аппаратное и программное обеспечение, а также сетевая конфигурация узлов кластера Kubernetes необходимым условиям для установки решения. Если все строгие предварительные проверки успешно завершены, KDT выводит уведомление об успешной проверке в stdout и журналы KDT. В противном случае сохраняются журналы с информацией о неудачной проверке и процесс добавления новых устройств прерывается. Вы можете пропустить предварительные проверки перед выполнением команды, если это необходимо (укажите для параметра установки `ignore_precheck` значение `true`).

Новые управляющие и рабочие узлы будут добавлены в кластер Kubernetes. KDT выводит информацию о добавленных управляющих и рабочих узлах в stdout и в журналы KDT.

Удаление управляющих и рабочих узлов из кластера Kubernetes

При удалении узлов нужно учитывать, что минимально допустимое количество управляющих узлов в кластере – один, а рабочих узлов – три. Если при удалении останется менее одного управляющего и трех рабочих узлов, операция будет прервана. Количество управляющих и рабочих узлов можно просмотреть в конфигурационном файле, который будет получен после экспорта.

Чтобы удалить управляющий и рабочие узлы:

1. На устройстве администратора экспортируйте текущий конфигурационный файл с помощью следующей команды:

   ```
   ./kdt ec -e '<имя_конфигурационного_файла_и_путь>'
   ```

   Текущая версия конфигурационного файла сохраняется в указанной директории с указанным именем.

2. В разделе `nodes` экспортированного конфигурационного файла удалите параметры одного или нескольких рабочих узлов (`desc`, `type`, `host`, `kind`, `user` и `key`) и сохраните конфигурационный файл.

Убедитесь, что после удаления узлов в кластере остался хотя бы один управляющий узел и не менее трех рабочих узлов. Минимальная конфигурация кластера для развертывания на нескольких узлах содержит четыре узла (один управляющий узел и три рабочих узла). Если это условие не выполняется, процесс удаления прерывается.

Вы также можете удалить узел с `kind=admsrv`, если это не единственный оставшийся узел с `kind=admsrv` в кластере. Если вы попытаетесь удалить этот узел из кластера, он будет пропущен в процессе удаления.

3. На устройстве администратора выполните следующую команду, чтобы применить измененный конфигурационный файл к кластеру Kubernetes. В команде укажите полный путь к этому конфигурационному файлу:

   ```
   ./kdt apply -i '<полный_путь_к_конфигурационному_файлу>'
   ```

   Указанные узлы удалены. KDT выводит информацию об удаленных управляющих и рабочих узлах в stdout и в журналы KDT.

Контроль версий конфигурационного файла

При работе с Kaspersky EDR Expert вам может потребоваться изменить параметры, которые были указаны в конфигурационном файле перед развертыванием Kaspersky EDR Expert. Например, чтобы изменить объем дискового пространства, используемого для хранения данных Сервера администрирования, нужно изменить параметр `ksc_state_size`. Текущая версия конфигурационного файла с измененным параметром `ksc_state_size` обновляется в кластере Kubernetes.

Если вы попытаетесь использовать предыдущую версию конфигурационного файла в пользовательском действии KDT, для которого требуется конфигурационный файл, возникнет конфликт. Чтобы избежать конфликтов, вам нужно использовать только текущую версию конфигурационного файла, экспортированного из кластера Kubernetes.

Чтобы экспортировать текущую версию конфигурационного файла,

на устройстве администратора, на котором расположена утилита KDT, запустите следующее пользовательское действие и укажите путь к конфигурационному файлу и его имя:

```
./kdt ec -e <имя_конфигурационного_файла_и_путь>
```

Текущая версия конфигурационного файла сохраняется в указанной директории с указанным именем.

Вы можете использовать экспортированный конфигурационный файл, например, при обновлении компонентов Kaspersky EDR Expert или добавлении плагинов управления для программам "Лаборатории Касперского".

Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.

Удаление Kaspersky EDR Expert

KDT позволяет вам удалить все компоненты Kaspersky EDR Expert установленные в кластере Kubernetes, сам кластер, сервисы KUMA, установленные вне кластера, и другие артефакты, созданные во время развертывания или работы решения.

Чтобы удалить компоненты Kaspersky EDR Expert и связанные с ними данные:

1. На устройстве администратора выполните следующую команду:

   ```
   ./kdt remove --all
   ```

   Эта команда удаляет следующие объекты и артефакты:

   - Все компоненты Kaspersky EDR Expert, установленные в кластере Kubernetes, и сам кластер.
   - Учетную запись пользователя Kaspersky EDR Expert, которая была создана с помощью KDT во время развертывания.
   - Базу данных, расположенную на отдельном сервере или внутри кластера, схемы СУБД и учетные записи СУБД, созданные с помощью KDT во время развертывания.
   - Сервисы KUMA, установленные вне кластера на устройствах, которые указаны в файле инвентаря.
   - Содержимое следующих директорий на целевых устройствах:
     - `/var/spool/ksc/logs`
     - `/var/spool/ksc/backup`
     - `/var/spool/ksc/`
     - `/var/lib/k0s`
     - `/run/k0s`
     - `/etc/k0s/`
     - `/etc/containerd/`
     - `/var/lib/containerd/`
     - `/run/containerd/`
   - Журналы событий, полученные во время установки и работы компонентов Kaspersky EDR Expert.
   - Данные, относящиеся к компонентам Kaspersky EDR Expert на устройстве администратора.

   Если устройство администратора не имеет сетевого доступа к целевому устройству, удаление компонентов прерывается. Вы можете восстановить доступ к сети и перезапустить удаление Kaspersky EDR Expert. Также вы можете удалить компоненты Kaspersky EDR Expert с целевых устройств вручную.

Если вы используете несколько кластеров Kubernetes, управляемых контекстами, эта команда удаляет только текущий контекст Kubernetes, соответствующий кластер и компоненты Kaspersky EDR Expert, установленные в кластере. Другие контексты и их кластеры с экземплярами Kaspersky EDR Expert не удаляются.

2. Закройте порты, используемые Kaspersky EDR Expert, которые были открыты при развертывании, если это необходимо. Эти порты не закрываются автоматически.

3. При необходимости удалите пакеты операционной системы, которые были автоматически установлены во время развертывания. Эти пакеты не удаляются автоматически.

4. Удалите KDT и содержимое директорий `~/kaspersky_eula` и `~/.kdt`.

Компоненты Kaspersky EDR Expert, база данных и связанные с ними данные будут удалены, а порты, используемые Kaspersky EDR Expert, закрыты.

Установленные на управляемых устройствах приложения "Лаборатории Касперского" невозможно удалить с помощью команды `./kdt remove`. Подробнее об удалении приложений "Лаборатории Касперского" см. в документации к ним.

После удаления Kaspersky EDR Expert, целевые устройства не перезагружаются автоматически. При необходимости вы можете перезагрузить эти устройства вручную.

Удаление компонентов Kaspersky EDR Expert вручную

Если устройство администратора не имеет сетевого доступа к целевому устройству, удаление компонентов Kaspersky EDR Expert с помощью KDT прерывается. Вы можете восстановить доступ к сети и перезапустить удаление решения. Также вы можете удалить компоненты Kaspersky EDR Expert с целевых устройств вручную.

Чтобы удалить компоненты Kaspersky EDR Expert с целевых устройств вручную:

1. На целевом устройстве остановите службу k0s с помощью команды:

   ```
   /usr/local/bin/k0s stop
   ```

2. Сбросьте узлы кластера в исходное состояние с помощью команды:

   ```
   /usr/local/bin/k0s reset
   ```

3. Удалите содержимое следующих директорий:

   - Обязательные директории:

     - `/etc/k0s/`
     - `/var/lib/k0s/`
     - `/usr/libexec/k0s/`
     - `/usr/local/bin/` (удалите только файл `k0s`)

- Необязательные директории:
  - `/var/lib/containerd/`
  - `/var/cache/k0s/`
  - `/var/cache/kubelet/`
  - `/var/cache/containerd/`

  Вы можете удалить директории `/var/lib/containerd/` и `/var/cache/containerd/`, если служба containerd используется только для работы Kaspersky EDR Expert. Иначе ваши данные, содержащиеся в директориях `/var/lib/containerd/` и `/var/cache/containerd/`, могут быть потеряны.

  Содержимое директорий `/var/cache/k0s/`, `/var/cache/kubelet/` и `/var/cache/containerd/` автоматически удаляется после перезапуска целевого устройства. Вам не нужно удалять содержимое этих директорий вручную.

4. Перезагрузите все целевые устройства.

Компоненты Kaspersky EDR Expert удалены с целевых устройств.

Переустановка Kaspersky EDR Expert после неудачной установки

Если не удалось установить Kaspersky EDR Expert, вы можете перезапустить установку. Сбой установки может возникнуть во время установки компонента Bootstrap или установки компонентов Kaspersky EDR Expert. Действия необходимые для переустановки Kaspersky EDR Expert зависят от того, был ли развернут кластер Kubernetes на момент возникновения ошибки установки.

Чтобы определить шаг, на котором не удалось выполнить установку,

выполните команду для просмотра списка всех установленных компонентов Kaspersky EDR Expert:

```
./kdt state
```

Если возникла ошибка установки Bootstrap, KDT выводит сообщение о том, что Bootstrap не установлен. В этом случае вам нужно вручную удалить директории, созданные во время развертывания.

Если компонент Bootstrap установлен, в выводе команды будет указан статус `Success`. Это означает, что произошла ошибка установки компонентов Kaspersky EDR Expert. В этом случае вам нужно переустановить неправильно установленные компоненты или переустановить все решение. В выводе команды такие компоненты имеют статус `Failed`.

Переустановка Kaspersky EDR Expert, если не установлен компонент Bootstrap

Чтобы начать установку заново Kaspersky EDR Expert:

1. Перейдите в директорию с утилитой KDT и просмотрите журнал событий установки компонента Bootstrap.

   Если на этапе установки Bootstrap произошел сбой, это будет отражено в журнале событий. В этом случае Bootstrap не установлен и кластер Kubernetes не создан.

   Выполните команду `/.kdt/kdt-{date}.log | grep -iE "connect|auth|ident|password"`, чтобы найти записи журнала, связанные с наиболее распространенными проблемами при установке:

   - Параметры подключения к базе данных
   - Формат пароля администратора
   - Недостаточно аппаратных ресурсов
   - Проблемы с авторизацией при подключении к узлам

2. Удалите вручную директории, созданные во время развертывания.

   a. На устройстве администратора перейдите в директорию `.kdt` и удалите файл `cluster.config`.

   b. Удалите содержимое следующих директорий:

      - Обязательные директории:
        - `/etc/k0s/`
        - `/var/lib/k0s/`
        - `/usr/libexec/k0s/`
        - `/usr/local/bin/` (удалите только файл `k0s`)
      - Необязательные директории:
        - `/var/lib/containerd/`
        - `/var/cache/k0s/`
        - `/var/cache/kubelet/`
        - `/var/cache/containerd/`

      Вы можете удалить директории `/var/lib/containerd/` и `/var/cache/containerd/`, если служба containerd используется только для работы Kaspersky EDR Expert. Иначе данные в директориях `/var/lib/containerd/` и `/var/cache/containerd/` могут быть потеряны.

Содержимое директорий `/var/cache/k0s/`, `/var/cache/kubelet/` и `/var/cache/containerd/` автоматически удаляется после перезапуска целевого устройства. Вам не нужно удалять содержимое этих директорий вручную.

c. Перезагрузите все целевые устройства.

3. Перезапустите установку Kaspersky EDR Expert.

Переустановка Kaspersky EDR Expert, если установлен компонент Bootstrap

Чтобы переустановить неправильно установленные компоненты Kaspersky EDR Expert:

1. Просмотрите полный журнал событий установки неправильно установленного компонента Kaspersky EDR Expert с помощью команды:

   ```
   ./kdt state -l <название_компонента>
   ```

   Также можно вывести всю диагностическую информацию о компонентах Kaspersky EDR Expert с помощью команды:

   ```
   ./kdt logs get --to-archive
   ```

2. Устраните ошибку установки самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

3. Переустановите неправильно установленные компоненты Kaspersky EDR Expert.

   - Если вы не изменяли конфигурационный файл, выполните следующую команду и укажите тот же транспортный архив, который использовался при установке Kaspersky EDR Expert:

     ```
     ./kdt apply -k <полный_путь_к_транспортному_архиву>
     ```

   - Если вам нужно изменить параметры установки, экспортируйте конфигурационный файл, измените его, а затем выполните следующую команду с транспортным архивом и обновленным конфигурационным файлом:

     ```
     ./kdt apply -k <полный_путь_к_транспортному_архиву> -i
     <полный_путь_к_конфигурационному_файлу>
     ```

   KDT переустанавливает только неправильно установленные компоненты Kaspersky EDR Expert.

4. Переустановите Kaspersky EDR Expert с помощью команды:

   ```
   ./kdt apply --force -k <полный_путь_к_архиву_обновлений_XDR> -i
   <полный_путь_к_конфигурационному_файлу>
   ```

Если переустановка компонентов не помогла устранить ошибку установки, вы можете удалить все решение.

Чтобы начать установку заново Kaspersky EDR Expert:

1. Выведите всю диагностическую информацию о компонентах Kaspersky EDR Expert с помощью команды:

   ```
   ./kdt logs get --to-archive
   ```

2. Устраните ошибку установки самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

3. Удалите Kaspersky EDR Expert. На устройстве администратора выполните команду:

```
./kdt remove --all
```

4. Переустановите Kaspersky EDR Expert с помощью команды:

```
./kdt apply --force -k <полный_путь_к_архиву_обновлений_XDR> -i
<полный_путь_к_конфигурационному_файлу>
```

Переустановка компонентов Kaspersky EDR Expert

Во время установки Kaspersky EDR Expert на устройстве администратора KDT отображает журнал событий установки, в котором видно, правильно ли установлены компоненты Kaspersky EDR Expert.

После установки Kaspersky EDR Expert вы можете запустить следующую команду, чтобы просмотреть список всех установленных компонентов:

```
./kdt state
```

Отображается список установленных компонентов. Правильно установленные компоненты имеют статус `Успешно`. Если не удалось установить компонент, этот компонент будет иметь статус `Сбой`.

Чтобы просмотреть полный журнал событий установки неправильно установленного компонента Kaspersky EDR Expert, выполните команду:

```
./kdt state -l <название_компонента>
```

Также можно вывести всю диагностическую информацию о компонентах Kaspersky EDR Expert с помощью следующей команды:

```
./kdt logs get --to-archive
```

Вы можете использовать полученные журналы событий для устранения неполадок самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Чтобы переустановить неправильно установленные компоненты Kaspersky EDR Expert:

- Если вы не изменяли конфигурационный файл, выполните следующую команду и укажите тот же транспортный архив, который использовался при установке Kaspersky EDR Expert:

  ```
  ./kdt apply -k <полный_путь_к_транспортному_архиву>
  ```

- Если вам нужно изменить параметры установки, экспортируйте конфигурационный файл, измените его, а затем выполните следующую команду с транспортным архивом и обновленным конфигурационным файлом:

  ```
  ./kdt apply -k <полный_путь_к_транспортному_архиву> -i
  <полный_путь_к_конфигурационному_файлу>
  ```

KDT переустанавливает только неправильно установленные компоненты Kaspersky EDR Expert.

Остановка узлов кластера Kubernetes

Вам может потребоваться остановить весь кластер Kubernetes или временно выключить один из узлов кластера для обслуживания.

В виртуальной среде не выключайте виртуальные машины, на которых размещены активные узлы кластера Kubernetes.

Если у вас нет прав суперпользователя, нужно получить их или повысить свои привилегии, добавив к каждой команде префикс `sudo`, например: `sudo k0s status`, `sudo k0s stop`.

Для получения полной информации о необходимых командах рекомендуется обратиться к официальной документации вашей операционной системы.

Остановка работы кластера Kubernetes на нескольких узлах

Чтобы остановить многоузловой кластер Kubernetes (схема развертывания на нескольких узлах):

1. Войдите на рабочий узел и инициируйте плавное завершение работы:

   a. Остановите узел, выполнив команду:

   ```
   k0s stop
   ```

   b. Проверьте, остановлен ли узел, выполнив команду:

   ```
   k0s status
   ```

   c. Завершите работу узла, выполнив команду:

   ```
   shutdown -now
   ```

   По соображениям безопасности не рекомендуется использовать ключи `--force`.

2. Повторите этот процесс для всех рабочих узлов.

3. Войдите в систему на управляющем узле и инициируйте плавное завершение работы, как описано в шагах a–c.

Если количество активных узлов в кластере Kubernetes падает ниже трех, до восстановления исходного количества узлов может произойти частичная потеря функциональности.
При выключении управляющего узла возможность управления кластером (в том числе с помощью утилиты kdt) будет потеряна до перезагрузки управляющего узла.

Остановка работы кластера Kubernetes на одном узле

Чтобы остановить кластер Kubernetes с одним узлом (схема развертывания на одном узле),

Войдите в систему на управляющем узле и инициируйте плавное завершение работы, как описано в шагах a–c.

Запуск кластера Kubernetes

Чтобы запустить кластер Kubernetes:

1. После загрузки операционной системы выполните команду:

   ```
   k0s start
   ```

2. Проверьте, запущен ли узел, выполнив команду:

   ```
   k0s status
   ```

3. Для развертывания на нескольких узлах повторите те же действия для их всех.

Использование сертификатов для публичных служб Kaspersky EDR Expert

Для работы с публичными службами Kaspersky EDR Expert вы можете использовать самоподписанные или пользовательские сертификаты. По умолчанию Kaspersky EDR Expert использует самоподписанные сертификаты.

Сертификаты необходимы для следующих публичных служб Kaspersky EDR Expert:

- `<console_host>.<smp_domain>` – доступ к интерфейсу Консоли OSMP.
- `<ksc_host>.<smp_domain>` – взаимодействие с Сервером администрирования.
- `<api_host>.<smp_domain>` – доступ к API Kaspersky EDR Expert.
- `<monitoring_host>.<smp_domain>` – доступ к метрикам OSMP.
- `<kuma_host>.<smp_domain>` – доступ к компоненту SIEM.

FQDN публичных служб Kaspersky EDR Expert состоят из имен устройств и доменного имени, указанных в конфигурационном файле. Список адресов публичных служб Kaspersky EDR Expert, для которых при развертывании определяются самоподписанные или пользовательские сертификаты, указывается в параметре установки `pki_host_list`.

Пользовательский сертификат должен быть указан как файл в формате PEM, содержащий полную цепочку сертификатов (или только один сертификат) и незашифрованный закрытый ключ.

Вы можете указать промежуточный сертификат из инфраструктуры закрытых ключей (PKI) вашей организации. Пользовательские сертификаты для публичных служб Kaspersky EDR Expert выдаются из этого пользовательского промежуточного сертификата. Также вы можете указать конечные сертификаты для каждой публичной службы. Если конечные сертификаты указаны только для части публичных служб, то для остальных публичных служб выдаются самоподписанные сертификаты.

Для публичных служб `<console_host>.<smp_domain>`, `<kuma_host>.<smp_domain>`, `<monitoring_host>.<smp_domain>`, и `<api_host>.<smp_domain>` пользовательские сертификаты можно указать только перед развертыванием в конфигурационном файле. Чтобы использовать пользовательский промежуточный сертификат, укажите параметры установки `intermediate_bundle` и `intermediate_enabled`. Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.

Если для работы с публичными службами Kaspersky EDR Expert требуется использовать пользовательские конечные сертификаты, укажите соответствующие параметры установки `console_bundle`, `admsrv_bundle`, `kuma_bundle`, `monitoring_bundle`, и `api_bundle`. Установите для параметра `intermediate_enabled` значение `false` и не указывайте параметры `intermediate_bundle` и `pki_host_list`. Максимальный срок действия пользовательского конечного сертификата должен быть 399 дней или больше.

Для службы `<ksc_host>.<smp_domain>` вы можете заменить выданный самоподписанный сертификат Сервера администрирования пользовательским сертификатом с помощью утилиты klsetsrvcert.

> Автоматический перевыпуск сертификатов не поддерживается. Примите во внимание срок действия сертификата и обновите сертификат, когда срок его действия истечет.

Чтобы обновить пользовательские сертификаты:

1. На устройстве администратора выполните экспорт текущей версии конфигурационного файла.
2. В экспортированном конфигурационном файле укажите путь к новому пользовательскому промежуточному сертификату в параметре установки `intermediate_bundle`. Если вы используете конечные пользовательские сертификаты для каждой публичной службы, укажите параметры установки `console_bundle`, `admsrv_bundle`, `kuma_bundle`, `monitoring_bundle` и `api_bundle`.
3. Выполните следующую команду и укажите полный путь к измененному конфигурационному файлу:

   ```
   ./kdt apply -i <полный_путь_к_конфигурационному_файлу>
   ```

   Пользовательские сертификаты обновлены.

Расчет и изменение дискового пространства для хранения данных Сервера администрирования

Данные Сервера администрирования включают в себя следующие объекты:

- Информация об активах (устройствах).
- Информация о событиях, зарегистрированных на Сервере администрирования для выбранного клиентского устройства.
- Информация о домене, в котором находятся активы.

- Данные компонента Контроль приложений.
- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

Расчет минимального дискового пространства для хранения данных Сервера администрирования

Минимальный объем дискового пространства, необходимый для хранения данных Сервера администрирования, можно приблизительно оценить по формуле:

```
(724 * C + 0.15 * E + 0.17 * A + U), КБ
```

где:

- C – количество активов (устройств).
- E – количество сохраняемых событий.
- A – суммарное количество объектов домена:
  - учетных записей устройств;
  - учетные записи пользователей;
  - учетных записей групп безопасности;
  - организационных подразделений.
- U – размер обновлений (не менее 4 ГБ).

Если опрос домена выключен, то "A" следует считать равным нулю.

Формула рассчитывает объем дискового пространства, необходимый для хранения типичных данных с управляемых устройств, и типичный размер обновлений. В формулу не входит объем дискового пространства, занятого данными, которые не зависят от количества управляемых устройств для компонента Контроль приложений, инсталляционных пакетов и задач удаленной установки.

Изменение дискового пространства для хранения данных Сервера администрирования

Объем свободного дискового пространства, выделяемого для хранения данных Сервера администрирования, указывается в конфигурационном файле перед развертыванием Kaspersky EDR Expert (параметр `ksc_state_size`). Примите во внимание минимальное дисковое пространство, рассчитанное по формуле.

Чтобы проверить объем дискового пространства, используемого для хранения данных Сервера администрирования после установки Kaspersky EDR Expert:

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke ksc --action getPvSize
```

Отображается объем необходимого свободного места на диске в гигабайтах.

Чтобы изменить объем дискового пространства для хранения данных Сервера администрирования после установки Kaspersky EDR Expert:

на устройстве администратора, на котором расположена утилита KDT, выполните команду, указав необходимое свободное место на диске в гигабайтах (например, "50Gi"):

```
./kdt invoke ksc --action setPvSize --param
ksc_state_size='<новый_объем_дискового_пространства>Gi'
```

Объем свободного дискового пространства, выделяемого для хранения данных Сервера администрирования, изменен.

Просмотр и изменение дискового пространства для Ядра KUMA и сервиса Метрики

Вы можете просмотреть текущий объем дискового пространства, выделенного для работы Ядра KUMA и сервиса Метрики. При необходимости вы можете изменить выделенное дисковое пространство.

Просмотр текущего выделенного дискового пространства

Команды для просмотра дискового пространства не влияют на работу запущенных служб.

Чтобы просмотреть дисковое пространство, выделенное для Ядра KUMA:

На устройстве администратора выполните команду:

```
./kdt invoke kuma --action getCorePvcSize
```

Чтобы просмотреть дисковое пространство, выделенное для сервиса Метрики:

На устройстве администратора выполните команду:

```
./kdt invoke kuma --action getMetricsPvcSize
```

Изменение текущего выделенного дискового пространства

Команды изменяют параметры `core_disk_request` и `metrics_disk_request`. Когда вы запускаете команду, соответствующая служба останавливается, дисковое пространство изменяется, служба перезапускается. Приложение обновляет параметры `core_disk_request` и `metrics_disk_request` только в случае успешного выполнения команд.

Вы можете только увеличить текущее дисковое пространство. Если вы попытаетесь установить значение дискового пространства меньше текущего, команда вернет ошибку. В этом случае службы не останавливаются.

Если ошибка возникает после того, как службы уже были остановлены, приложение пытается перезапустить службы и сохранить предыдущее значение дискового пространства.

Чтобы изменить дисковое пространство, выделенное для Ядра KUMA:

На устройстве администратора выполните команду:

```
./kdt invoke kuma --action setCorePvcSize --param core_disk_request=<значение>
```

где `<значение>` – новый размер дискового пространства, например `50Gi`.

Чтобы изменить дисковое пространство, выделенное для сервиса Метрики:

На устройстве администратора выполните команду:

```
./kdt invoke kuma --action setMetricsPvcSize --param metrics_disk_request=<значение>
```

где `<значение>` – новый размер дискового пространства, например `50Gi`.

Просмотр и изменение размера объектного хранилища

Объектное хранилище – это компонент для хранения временных данных плейбуков, файлов алертов и инцидентов, а также поддержки S3 API для внешних интеграций. Если том объектного хранилища заполняется, вы можете проверить текущий выделенный размер для него. Изменить размер хранилища можно с помощью утилиты KDT. Это предотвращает переполнение хранилища и связанное с ним нарушение работы сервиса.

Чтобы проверить размер объектного хранилища:

На устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke objectstorage --action getDataPvSize
```

В выводе команды отображается текущий выделенный размер объектного хранилища в гигабайтах (например, 10Gi).

Чтобы увеличить размер объектного хранилища:

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke objectstorage --action setDataPvSize --param volumeDataSize=<новый_размер>
```

где `<новый_размер>` – требуемый размер объектного хранилища в гигабайтах (например, 11Gi). Значение должно быть больше текущего размера.

Размер объектного хранилища изменен. Новый размер объектного хранилища становится доступным без перезапуска сервиса.

Увеличение размера хранилища наблюдаемости

Компонент наблюдаемости – это компонент, который обеспечивает централизованную видимость событий, угроз и активов. KDT позволяет увеличить размер хранилища для компонента наблюдаемости (VictoriaMetrics).

Чтобы увеличить размер хранилища для компонента наблюдаемости вручную,

На устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke observability --action increaseVMPvSize --param prometheus_size=<new_size>
```

где `<new_size>` – требуемый размер хранилища в гигабайтах (например, 11Gi). Значение должно быть больше текущего размера.

Размер хранилища для компонента наблюдаемости изменен до указанного значения.

Ротация сертификатов кластера Kubernetes

KDT позволяет чередовать сертификаты кластера Kubernetes, которые обеспечивают доступ к кластеру Kubernetes и компонентам инфраструктуры Kaspersky EDR Expert. Сертификаты кластера Kubernetes расположены на целевых устройствах внутри кластера Kubernetes.

Чтобы чередовать сертификаты кластера Kubernetes вручную:

На устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke foreach --action RotateK0sConfig
```

После чего будут созданы новые сертификаты кластера Kubernetes. По умолчанию срок чередования составляет 10 лет.

При обновлении Bootstrap сертификаты кластера Kubernetes обновляются автоматически.

Ротация учетных данных для доступа к реестру

KDT позволяет вам выполнять ротацию учетных данных для доступа к реестру в соответствии с требованиями к информационной безопасности вашей организации.

Чтобы сменить учетные данные для доступа к реестру вручную,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke bootstrap --action RotateRegistryCreds
```

Учетные данные для доступа к реестру обновлены.

При обновлении Bootstrap учетные данные для доступа к реестру обновляются автоматически.

Ротация учетных данных СУБД и сертификатов

KDT позволяет менять учетные данные СУБД и сертификаты, используемые для подключения к СУБД. Вы можете выполнять ротацию секретов СУБД в соответствии с требованиями к информационной безопасности вашей организации.

Чтобы выполнить ротацию учетных данных СУБД и сертификатов вручную,

На устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke foreach --action rotatedbcreds
```

обновите учетные данные СУБД и сертификаты.

Добавление устройств для установки дополнительных сервисов KUMA

Если вам нужно расширить хранилище или добавить коллекторы и корреляторы для увеличения потока событий, вы можете добавить дополнительные устройства для установки сервисов KUMA.

Вам нужно указать параметры дополнительных устройств в файле expand.inventory.yml. Этот файл находится в дистрибутиве с транспортным архивом, KDT, конфигурационным файлом и другими файлами. В файле expand.inventory.yml можно указать сразу несколько дополнительных устройств для коллекторов, корреляторов и хранилищ. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке на выбранных устройствах.

Чтобы подготовить требуемую инфраструктуру на устройствах, указанных в файле expand.inventory.yml, вам нужно создать служебные директории, в которые будут добавлены файлы, необходимые для установки службы. Чтобы подготовить инфраструктуру, выполните следующую команду и укажите файл expand.inventory.yml:

```
./kdt invoke kuma --action addHosts --param host_inventory='<путь_к_файлу_инвентаря>'
```

На устройствах, указанных в файле expand.inventory.yml, служебные каталоги, в которые добавляются файлы, необходимые для установки службы.

Пример дополнительного файла инвентаря KUMA для установки сервисов KUMA (файл expand.inventory.yml)

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
    kuma_collector:
      hosts:
        kuma1.example.com:
            ansible_host: 0.0.0.0
        kuma2.example.com:
            ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma3.example.com:
            ansible_host: 0.0.0.0
        kuma4.example.com:
            ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma5.example.com:
            ansible_host: 0.0.0.0
        kuma6.example.com:
            ansible_host: 0.0.0.0
```

Добавление дополнительного хранилища, коллектора или коррелятора

Вы можете добавить к существующей инфраструктуре дополнительное хранилище кластера, коллектор или коррелятор. Если вы хотите добавить несколько сервисов, рекомендуется устанавливать их в следующем порядке: хранилища, коллекторы и корреляторы.

Чтобы добавить дополнительное хранилище кластера, коллектор или коррелятор:

1. В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.

2. В разделе KUMA Консоли OSMP создайте набор ресурсов для каждого сервиса KUMA (хранилищ, коллекторов и корреляторов), который вы хотите установить на подготовленных устройствах.

3. Создайте сервисы для хранилищ, коллекторов и корреляторов.

4. Получите идентификаторы сервисов для привязки созданных наборов ресурсов и сервисов KUMA:

   a. В главном окне решения OSMP перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. Установите сервисы KUMA на каждое подготовленное устройство, указанное в разделах kuma_storage, kuma_collector и kuma_correlator файла инвентаря expand.inventory.yml. На каждом устройстве в команде установки укажите идентификатор сервиса, соответствующий устройству. Выполните соответствующие команды, чтобы установить сервисы KUMA:

   - Команда установки хранилища:

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the
     KUMA Core CA certificate> --id <service ID> --install
     ```

   - Команда установки коллектора:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port>
     ```

   - Команда установки коррелятора:

     ```
     sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
     ```

   Команды установки коллектора и коррелятора автоматически создаются на вкладке **Проверка** в мастере установки. Порт, используемый для связи, автоматически добавляется в команду. Используйте сгенерированные команды для установки коллектора и коррелятора на устройства. Это позволит убедиться, что порты для связи с сервисами, которые указаны в команде, доступны.

где:

- <FQDN> – полное доменное имя сервера Ядра KUMA. FQDN Ядра KUMA – это <kuma_host>.<smp_domain>. Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

- <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

Дополнительные сервисы KUMA установлены.

Добавление устройств в существующее хранилище

Вы можете расширить существующее хранилище (хранилище кластера), добавив устройства в качестве новых узлов хранилища кластера.

Чтобы добавить устройства в существующее хранилище:

1. В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.
2. Добавьте узлы в хранилище кластера. Для этого измените параметры существующего хранилища кластера:
   a. В разделе **Ресурсы** → **Хранилища** выберите существующее хранилище и откройте хранилище для изменения.
   b. В разделе **Узлы кластера ClickHouse** нажмите на **Добавить узлы** и в полях для нового узла укажите роли. Укажите соответствующие доменные имена устройств из раздела kuma_storage файла expand.inventory.yml, а затем укажите роли для новых узлов.
   c. Сохраните изменения.

   Поскольку вы добавляете серверы в существующий кластер хранилища, создавать отдельное хранилище уже не нужно.
3. Создайте сервисы хранилища для каждого добавленного узла хранилища кластера в разделе KUMA Консоли OSMP и привяжите сервисы к хранилищу кластера.
4. Получите идентификаторы сервиса хранилища для каждого подготовленного устройства для установки сервисов KUMA:
   a. В разделе KUMA Консоли OSMP перейдите в раздел **Ресурсы** → **Активные сервисы**.
   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. Установите сервис хранилища на каждое подготовленное устройство, указанное в разделе kuma_storage файла инвентаря expand.inventory.yml. На каждом устройстве в команде установки укажите идентификатор сервиса, соответствующий устройству. Выполните следующую команду, чтобы установить сервис хранилища:

```
sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA
Core CA certificate> --id <service ID> --install
```

где:

- <FQDN> – полное доменное имя сервера Ядра KUMA. FQDN Ядра KUMA – это <kuma_host>. <smp_domain>. Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

- <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

  Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

  Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.

Дополнительные устройства добавлены в хранилище кластера.

Укажите добавленные устройства в файле инвентаря distributed.inventory.yml, чтобы в нем были актуальные сведения на случай обновления компонентов KUMA.

Замена устройства, использующего хранилище KUMA

Чтобы заменить устройство, использующее хранилище KUMA, на другое:

1. Заполните файл expand.inventory.yml, указав параметры устройства, которое вы хотите заменить.

2. Выполните следующую команду, указав файл expand.inventory.yml для удаления устройства:

```
./kdt invoke kuma --action removeHosts --param
host_inventory='<путь_к_файлу_инвентаря>'
```

3. Заполните файл expand.inventory.yml, указав параметры нового устройства, которым вы хотите заменить предыдущее, и выполните команду:

   ```
   ./kdt invoke kuma --action addHosts --param host_inventory='<путь_к_файлу_инвентаря>'
   ```

4. Выполните шаги 2–6 инструкции по добавлению устройств для сервисов KUMA, чтобы добавить устройство с хранилищем KUMA.

Устройство с хранилищем KUMA заменено на другое.

Если ваша конфигурация хранилища включает в себя шард, содержащий две реплики, и вы заменили второе устройство реплики на новый, выполнив действия, описанные выше, то при установке новой реплики вы можете получить сообщение об ошибке. В этом случае новая реплика работать не будет.

Чтобы исправить ошибку при добавлении реплики шарда:

1. На другом устройстве с репликой того же шарда, которому принадлежит неправильно добавленная реплика, запустите клиент ClickHouse с помощью команды:

   ```
   /opt/kaspersky/kuma/clickhouse/bin/client.sh
   ```

   Если это устройство недоступно, запустите клиент на любом другом устройстве с репликой, включенной в то же хранилище кластера.

2. Запустите команду, чтобы удалить данные об устройстве, которое вы хотите заменить:

   - Если доступно устройство с репликой того же шарда, которому принадлежит неправильно добавленная реплика, выполните команду:

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM TABLE
     kuma.events_local_v2
     ```

   - Если вы используете другой узел хранилища кластера с репликой, выполните команду:

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM ZKPATH
     '/clickhouse/tables/kuma/<shard number of read-only node>/kuma/events_local_v2
     ```

3. Восстановите работу добавленного устройства с репликой с выполнив команду:

   ```
   SYSTEM RESTORE REPLICA kuma.events_local_v2
   ```

Работоспособность добавленного устройства с репликой восстановлена.

Работа с Kaspersky EDR Expert, развернутым на виртуальных машинах

Если вы развернули Kaspersky EDR Expert на виртуальных машинах, не рекомендуется делать снимки или переносить эти виртуальные машины с помощью гипервизора во время работы решения. В этом случае Kaspersky EDR Expert будет работать некорректно. Чтобы обеспечить правильную работу Kaspersky EDR Expert, вам нужно остановить все виртуальные машины в кластере Kubernetes перед созданием снимков или выполнением переноса данных.

Настройка модели статусов инцидентов

Поддерживаются две модели статусов инцидентов:

a. Стандартная:

- **Новый**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *В обработке*, инцидент назначается вам автоматически. Когда вы меняете статус *Новый* на *Закрыт* и у инцидента нет исполнителя, он автоматически назначается вам.

- **В обработке**

  Этот статус означает, что аналитик начал работу над алертом. Статус *В обработке* может быть изменен на *Новое* и *Закрыто*.

- **Отложен**

  Этот статус назначается алерту при привязке к инциденту. Этот статус нельзя выбрать вручную. Статус *Закрыто* может быть назначен только привязанному алерту. Чтобы сменить этот статус на *Новое* или *В обработке*, необходимо сначала отменить связь алерта с инцидентом.

- **Закрыт**

  Вы закрываете инциденты, когда не требуется никакой дополнительной работы над инцидентом. Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыто* и наследуют решение инцидента. Если у инцидента нет исполнителя, закрытый инцидент автоматически назначается вам. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый инцидент в работу, измените его статус следующим образом: *Закрыт* → *Новый* → *В обработке*.

b. Совместимая с ГОСТ:

- **Новый**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *Анализ*. Когда вы меняете статус *Новый* на *Анализ*, инцидент назначается вам автоматически.

- **Анализ**

  Этот статус означает, что аналитик начал работу над инцидентом и проводит первичный анализ и определение вовлеченных в инцидент элементов информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Локализация* или *Выполнен*.

- **Локализация**

  Этот статус означает, что выполняется меры по предотвращению дальнейшего распространения инцидента.

  Вы можете изменить статус инцидента на *Последствия* или *Выполнен*.

- **Последствия**

  Этот статус означает, что выполняется выявление последствий инцидента на вовлеченные в него элементы информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Ликвидация* или *Выполнен*.

- **Ликвидация**

  Этот статус означает, что выполняется устранение последствий инцидента.

  Вы можете изменить статус инцидента на *Выполнен*.

- **Выполнен**

  Этот статус означает, что проводится оценка полноты выполненных действий на этапах *Анализ*, *Локализация*, *Последствия* и *Ликвидация*.

  Вы можете изменить статус инцидента на *Закрыт*, *Анализ*, *Локализация*, *Последствия*, *Ликвидация*.

- **Закрыт**

  Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыт* и наследуют решение инцидента. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

Чтобы сменить модель статусов на совместимую с ГОСТ:

1. В файле docker/compose/osmp.yaml укажите значение переменной окружения OSMP_WORKFLOW_ID.

   OSMP_WORKFLOW_ID: "gost"

2. В файле /plugins/irp/.env укажите значение переменной FEATURE_GOST_STATUS.

   FEATURE_GOST_STATUS=true

Статусы инцидентов не конвертируются при смене модели статуса. Не рекомендуется менять модель статусов, если у вас есть активные инциденты.

Демонстрационное развертывание Kaspersky EDR Expert

Если вы хотите ознакомиться с Kaspersky EDR Expert, вы можете выполнить демонстрационное развертывание решения.

Используйте демонстрационное развертывание Kaspersky EDR Expert (в котором СУБД установлена в кластере Kubernetes) только для ознакомления с решением. Не рекомендуется использовать этот подход для решения стандартных рабочих задач. Для стандартного использования выполните развертывание на нескольких узлах или на одном узле.

При демонстрационном развертывании все компоненты Kaspersky EDR Expert устанавливаются на одном или на нескольких узлах кластера Kubernetes.

В приведенном ниже сценарии описано демонстрационное развертывание на одном узле. Развертывание на одном узле требует меньше ресурсов и поэтому чаще используется для демонстрационного развертывания. При демонстрационном развертывании на одном узле кластер Kubernetes, компоненты Kaspersky EDR Expert и СУБД устанавливаются на одном целевом устройстве. Кроме того, вам потребуется устройство администратора для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert, а также целевое устройство для установки сервисов KUMA.

В этой конфигурации на одном узле вам понадобится минимум три устройства:

- 1 устройство администратора;
- 1 целевое устройство для установки кластера Kubernetes, компонентов Kaspersky EDR Expert и СУБД;
- 1 целевое устройство KUMA для установки сервисов KUMA.

Основное отличие между демонстрационным развертыванием и стандартным заключается в расположении СУБД. В стандартной конфигурации (на нескольких узлах или одном узле), СУБД устанавливается на устройстве, расположенном за пределами кластера. В демонстрационном развертывании СУБД устанавливается на целевое устройство внутри кластера.

Прежде чем приступить к развертыванию Open Single Management Platform и компонентов Kaspersky EDR Expert, рекомендуется прочитать Руководство по усилению защиты.

Следуя этому сценарию, вы можете подготовить инфраструктуру для демонстрационного развертывания, подготовить конфигурационный файл и развернуть решение с помощью утилиты Kaspersky Deployment Toolkit (далее также KDT).

Сценарий демонстрационного развертывания состоит из следующих этапов:

1. **Загрузка дистрибутива с компонентами Kaspersky EDR Expert**

В состав дистрибутива входят следующие компоненты:

- Транспортный архив, который содержит компоненты Kaspersky EDR Expert и Лицензионные соглашения Kaspersky EDR Expert и KDT.

  Компоненты подписаны ключом RSA и ключом ГОСТ Р 34.11-2012.

- Архив с утилитой KDT, а также шаблоны конфигурационного файла и файл инвентаря KUMA.

2. **Подготовка устройства администратора и целевых устройств**

   Подготовьте выбранные устройство администратора и целевые устройства к демонстрационному развертыванию Kaspersky EDR Expert.

   Инструкция: Подготовка устройства администратора и целевых устройств.

3. **Подготовка устройств KUMA**

   Подготовьте целевые устройства KUMA для установки сервисов KUMA (коллекторы, корреляторы и хранилища).

   Инструкции: Подготовка устройств к установке сервисов KUMA.

4. **Подготовка файла инвентаря KUMA для установки сервисов KUMA**

   Подготовьте файл инвентаря KUMA в формате YAML. Файл инвентаря KUMA содержит параметры для установки сервисов KUMA

   Инструкции: Подготовка файла инвентаря KUMA.

5. **Подготовка конфигурационного файла**

   Подготовьте конфигурационный файл в формате YAML. Конфигурационный файл содержит параметры целевого устройства для развертывания и набор параметров для установки компонентов Kaspersky EDR Expert.

   Инструкции: Указание параметров установки.

6. **Развертывание Kaspersky EDR Expert**

   Разверните Kaspersky EDR Expert с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Kaspersky EDR Expert и другие компоненты инфраструктуры.

   Инструкции: Установка Kaspersky EDR Expert.

7. **Установка сервисов KUMA**

   Установите сервисы KUMA (коллекторы, корреляторы и хранилища) на подготовленные целевые устройства KUMA, расположенные вне кластера Kubernetes.

   Инструкции: Установка сервисов KUMA.

8. **Настройка интеграции с Kaspersky Anti Targeted Attack Platform**

   Установите Central Node, чтобы получать телеметрию от Kaspersky Anti Targeted Attack Platform, а затем настройте интеграцию Kaspersky EDR Expert и KATA/KEDR для управления действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response.

   При необходимости вы можете установить несколько компонентов Central Node, чтобы использовать их независимо друг от друга или объединить для централизованного управления в режиме распределенного решения. Чтобы объединить несколько компонентов Central Node, вам нужно организовать серверы с компонентами в иерархию.

При настройке серверов Central Node вам нужно указать минимально возможное значение в поле **Хранилище**, чтобы избежать дублирования данных между базами Kaspersky EDR Expert и KEDR.

Подготовка устройства администратора и целевых устройств

Подготовка к демонстрационному развертыванию на одном узле включает настройку устройства администратора и целевых устройств. При демонстрационном развертывании на одном узле кластер Kubernetes, компоненты Kaspersky EDR Expert и СУБД устанавливаются на одном целевом устройстве. После подготовки целевого устройства и указания конфигурационного файла, вы сможете развернуть Kaspersky EDR Expert на целевом устройстве с использованием KDT.

Используйте демонстрационное развертывание Kaspersky EDR Expert (в котором СУБД установлена в кластере Kubernetes) только для ознакомления с решением. Не рекомендуется использовать этот подход для решения стандартных рабочих задач.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert. В этом случае будет использовано только одно устройство для развертывания и работы решения.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям для KDT.

2. Выделите не менее 10 ГБ свободного места в директории временных файлов (по умолчанию `/tmp`) для KDT. Если у вас недостаточно свободного места в этой директории, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<новая_директория>/tmp
   ```

3. Настройте среду выполнения контейнера. Используйте один из следующих сред:

   - Встроенная среда выполнения контейнера KDT (на основе runc).

     Чтобы установить среду, выполните команду:

     ```
     sudo ./kdt init
     ```

     Если встроенная среда выполнения контейнера не подходит для вашего окружения, вы можете использовать вместо нее среда выполнения контейнера Docker.

   - Среда выполнения контейнера Docker.

Установите пакет для Docker версии 25 или выше. Не устанавливайте неофициальные версии пакета Docker из хранилищ операционных систем.

Если keyring Docker невозможно скачать автоматически, скачайте его вручную:

a. Откройте ссылку https://download.docker.com/linux/ubuntu/gpg в браузере и сохраните ключ как docker.asc.

b. Выполните следующую команду:

```
sudo mv docker.asc /etc/apt/keyrings/docker.asc
```

На разделе диска для хранения данных Docker (по умолчанию `/var/lib/docker`) должно быть не менее 60 ГБ свободного места.

Выполните действия после установки, чтобы настроить устройство администратора для правильной работы с Docker:

```
sudo groupadd docker
sudo usermod -aG docker $USER
newgrp docker
sudo systemctl enable docker.service
sudo systemctl enable containerd.service
sudo systemctl status docker.service
```

4. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Так как устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на одном узле.

   b. Убедитесь, что на устройстве администратора поддерживается технология cgroup v2.

Подготовка целевых устройств

Целевое устройство – это физическая или виртуальная машина, которая используются для развертывания Kaspersky EDR Expert и которая включена в кластер Kubernetes. Целевое устройство управляет кластером Kubernetes, хранит метаданные, а также на этом устройстве работают компоненты Kaspersky EDR Expert. Минимальная конфигурация кластера для демонстрационного развертывания с одним узлом включает одно целевое устройство, которое действует как управляющий и рабочий узлы. На этом первичном рабочем узле установлен кластер Kubernetes, СУБД и компоненты Kaspersky EDR Expert.

Сервисы KUMA (коллекторы, корреляторы и хранилища) могут быть установлены внутри кластера на основном рабочем узле, на отдельных устройствах вне кластера Kubernetes или частично в кластере Kubernetes и вне его.

Если вы хотите запустить развертывание Kaspersky EDR Expert с целевого устройства, вам нужно подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, а затем выполнить подготовку для целевого устройства.

Чтобы подготовить целевое устройство:

1. Убедитесь, что аппаратное и программное обеспечение на целевом устройстве соответствуют требованиям для развертывания на одном узле (поскольку демонстрационное развертывание и развертывание на одном узле имеют схожую схему развертывания).

   Если сервисы KUMA установлены в кластере, целевое устройство должно соответствовать требованиям к оборудованию, программному обеспечению и требованиям установки, необходимым для установки сервисов KUMA.

   > Для правильной работы Kaspersky EDR Expert версия ядра Linux должна быть 5.15.0.107 или выше на целевом устройстве с операционной системой семейства Ubuntu.

   > Для правильной работы кластера Kubernetes и его компонентов подкачка должна быть выключена на всех узлах кластера. Если на узле включена подкачка, KDT автоматически выключит ее во время развертывания.

   > Не устанавливайте Docker на целевом устройстве, если целевое устройство не будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. Убедитесь, что в файловой системе, смонтированной в `/var`, на целевом устройстве есть не менее 360 ГБ свободного дискового пространства.

   Рекомендуется разместить директорию `/opt/lvp/hot` в выделенной высокопроизводительной дисковой подсистеме, а директорию `/opt/lvp/cold` в отдельной высокоемкой дисковой подсистеме.

3. Установите пакет sudo, если этот пакет еще не установлен. Для операционных систем семейства Debian установите пакет UFW.

4. Настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, подключите целевое устройство к интернету.

5. На управляющем рабочем узле с конфигурацией UFW разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

6. Предоставьте доступ к хранилищу пакетов, в котором хранятся следующие пакеты, необходимые для Kaspersky EDR Expert:

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common

- open-iscsi
- python3-cffi-backend
- python3-cryptography
- python3-netaddr
- python-apt-common
- systemd
- tar

KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

7. Убедитесь, что на управляющем рабочем узле установлены следующие пакеты:

   - python3-apt
   - curl

   Эти пакеты не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены.

8. Зарезервируйте статические IP-адреса для целевых устройств и шлюза кластера Kubernetes.

   Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes.

   После того как вы устанавливаете СУБД внутри кластера Kubernetes, IP-адрес шлюза становится IP-диапазоном (например, 192.168.0.1–192.168.0.2). Первый IP-адрес диапазона – это адрес служб Kaspersky EDR Expert (без учета IP-адреса СУБД). Второй IP-адрес диапазона – IP-адрес СУБД.

   Убедитесь, что целевое устройство и шлюз соединения кластера Kubernetes находятся в одном широковещательном домене.

9. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Kaspersky EDR Expert.

   По умолчанию службы Kaspersky EDR Expert доступны по следующим адресам:

   - <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
   - <ksc_host>.<smp_domain> – взаимодействие с Сервером администрирования.
   - <kuma_host>.<smp_domain> – доступ к компоненту SIEM.
   - <api_host>.<smp_domain> – доступ к API Kaspersky EDR Expert.
   - <monitoring_host>.<smp_domain> – доступ к метрикам OSMP.

- <xdr_edr_ingress_host>.<smp_domain> – взаимодействие с Сервером агента.

  Где <console_host>, <ksc_host>, <kuma_host>, <api_host>, <monitoring_host>, и <xdr_edr_ingress_host> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями служб FQDN, которые вы можете указать в конфигурационном файле. Если вы не указываете пользовательские значения имен служб устройств, используются значения по умолчанию: `console_host` – `"console"`, `ksc_host` – `"admsrv"`, `kuma_host` – `"kuma"`, `api_host` – `"api"`, `monitoring_host` – `"monitoring"`, `"xdr_edr_ingress_host" - "agentserver"`.

Перечисленные FQDN служб должны разрешаться в IP-адрес кластера Kubernetes. Например, если адрес кластера Kubernetes – 10.80.23.182, FQDN служб должны разрешаться в IP-адрес следующим образом:

- <console_host>.<smp_domain> – 10.80.23.182
- <ksc_host>.<smp_domain> – 10.80.23.182
- <kuma_host>.<smp_domain> – 10.80.23.182
- <api_host>.<smp_domain> – 10.80.23.182
- <xdr_edr_ingress_host>.<smp_domain>—10.80.23.182

10. Создайте учетные записи, которые будут использоваться для развертывания Kaspersky EDR Expert.

    Эти учетные записи используются для SSH-соединения и должны иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

    Просмотреть информацию

    Чтобы добавить созданные учетные записи пользователей в файл `/etc/sudoers`:

    1. Выполните следующие команды:

       ```
       sudo useradd -m -s /bin/bash <имя_пользователя>
       sudo usermod -aG sudo <имя_пользователя>
       ```

    2. Откройте файл `/etc/sudoers` с помощью команды:

       ```
       sudo visudo
       ```

    3. Добавьте следующую строку в конец секции `# Allow members of group sudo to execute any command`:

       ```
       <имя_пользователя> ALL=(ALL) NOPASSWD: ALL
       ```

       Где `<имя_пользователя>` – имя созданного пользователя.

    4. Сохраните и закройте файл `/etc/sudoers`.

11. Настройте SSH-соединение между устройством администратора и целевыми устройствами:

    a. На устройстве администратора сгенерируйте SSH-ключи с помощью утилиты ssh-keygen без парольной фразы.

    b. Скопируйте открытый ключ на целевое устройство (например, в директорию `/home/<имя_пользователя>/.ssh`) с помощью утилиты ssh-copy-id.

    Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

12. Для корректной работы компонентов Kaspersky EDR Expert откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

13. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

14. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Kaspersky EDR Expert.

    Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации, или конечные сертификаты для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Указание параметров установки

Конфигурационный файл, используемый для развертывания Kaspersky EDR Expert на одном узле, содержит параметры установки, необходимые как для развертывания на нескольких узлах, так и для развертывания на одном узле. Также этот конфигурационный файл содержит параметры, специфичные для развертывания на одном узле (`openbao_ha_mode`, `openbao_standalone` и `default_class_replica_count`). Шаблон конфигурационного файла (singlenode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT. Этот конфигурационный файл можно использовать для демонстрационной установки.

Используйте демонстрационное развертывание Kaspersky EDR Expert (в котором СУБД установлена в кластере Kubernetes) только для ознакомления с решением. Не рекомендуется использовать этот подход для решения стандартных рабочих задач. Для стандартного использования выполните развертывание на нескольких узлах или на одном узле.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны перед развертыванием Kaspersky EDR Expert. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения. Значения параметров должны соответствовать описанным ниже правилам. Во время развертывания Kaspersky EDR Expert, KDT проверяет, правильно ли указаны нужные параметры установки. Если необходимые параметры в конфигурационном файле отсутствуют или недействительны, развертывание будет прервано.

Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Раздел `nodes` конфигурационного файла содержит параметры целевого устройства, которые перечислены в таблице ниже.

Раздел nodes

Имя параметра	Обязательная	Описание

`desc`	Да	Имя узла.
		Значение должно соответствовать следующим правилам:
		• Длина имени узла должна быть от 1 до 63 символов.
		• Имя узла может содержать следующие символы:
		  • символы ASCII верхнего регистра (A–Z);
		  • символы ASCII нижнего регистра (a-z);
		  • числа (0–9);
		  • дефис (-).
		Все узлы кластера должны иметь уникальные имена. Это требование является одним из обязательных для установки Kaspersky EDR Expert и проверяется с помощью KDT.

`type`	Да	Тип узла. Для целевого устройства для параметра `type` укажите значение `primary-worker`, чтобы включить **демонстрационное развертывание на одном узле**. В этом случае целевое устройство будет действовать как первичный и рабочий узлы.
`host`	Да	IP-адрес узла. Управляющий рабочий узел должен быть включен в ту же подсеть, что и шлюз кластера Kubernetes. Для узла требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера.
`kind`	Нет	Тип узла, определяющий компонент Kaspersky EDR Expert, который будет установлен на этом узле. Для **демонстрационного развертывания на одном узле** оставьте этот параметр пустым, поскольку все компоненты будут установлены на одном узле.

`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 31 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • нижнее подчеркивание (_), дефис (-).

`password`	Нет	Пароль для подключения к узлу. Может использоваться вместо SSH-ключа, указанного в параметре `ssh_pk`.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Раздел параметров

Имя параметра	Обязательная	Описание
`nwc-language`	Да	Язык интерфейса OSMP Console, указанный по умолчанию. После установки вы можете изменить язык OSMP Console. Возможные значения параметра: • `enUS` (значение по умолчанию) • `ruRu` Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.

Имя параметра	Обязательная	Описание
`ingress_ip`	Да	Зарезервированный статический IPv4-адрес шлюза кластера Kubernetes. Шлюз Kubernetes предназначен для подключения компонентов Kaspersky EDR Expert, установленных внутри кластера Kubernetes. Шлюз кластера должен быть включен в ту же подсеть, что и первичный рабочий узел кластера. Для шлюза кластера Kubernetes требуется IPv4-адресация. KDT самостоятельно отключает IPv6 на узлах кластера. В качестве значения этого параметра нельзя указывать IP-адрес того же устройства, на котором выполняется развертывание. При **демонстрационном развертывании**, когда СУБД устанавливается внутри кластера, IP-адрес СУБД совпадает с IP-адресом шлюза кластера.
`ssh_pk`	Да	Путь к закрытой части SSH-ключа, которая находится на устройстве администратора и используется для подключения к управляющему рабочему узлу и к узлам со службами KUMA (коллекторам, корреляторам и хранилищам) с помощью утилиты KDT. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64.
`admin_password`	Да	Параметр `admin_password` задает пароль Kaspersky EDR Expert, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 10 или более 256 символов. • Пароль должен содержать символы как минимум трех групп из списка ниже: • верхний регистр (A–Z); • нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;). • Пароль не должен содержать пробелов или комбинации ".@". Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера развертывания), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Да	Параметр, который указывает на то, что Kaspersky EDR Expert установлен на целевом устройстве с ограниченными вычислительными ресурсами. Для **демонстрационного развертывания на одном узле** для параметра `low_resources` установите значение `true`, чтобы компоненты Kaspersky EDR Expert требовали меньше ресурсов памяти и процессора. Если вы включите этот параметр, для установки Ядра KUMA на целевом устройстве будет выделено 4 ГБ свободного дискового пространства.
`openbao_ha_mode`	Да	Параметр, который указывает, следует ли запускать хранилище секретов в режиме High Availability (HA). Для **демонстрационного развертывания на одном узле** для параметра `openbao_ha_mode` установите значение `false`.
`openbao_standalone`	Да	Параметр, который указывает, следует ли запускать хранилище секретов в автономном режиме. Для **демонстрационного развертывания на одном узле** для параметра `openbao_standalone` установите значение `true`.
`default_class_replica_count`	Да	Количество дисковых томов, на которых хранятся служебные данные компонентов Kaspersky EDR Expert и KDT. По умолчанию указано значение `3`. Для **демонстрационного развертывания на одном узле** для параметра `default_class_replica_count` установите значение `1`.

Имя параметра	Обязательная	Описание
core_disk_request	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Если вы не укажете параметр core_disk_request, а для параметра low_resources установлено значение false или ничего не указано, для работы Ядра KUMA будет выделен объем дискового пространства 100 ГБ по умолчанию. Если вы не укажете параметр core_disk_request, а для параметра low_resources установлено значение true, для работы Ядра KUMA будет выделен объем дискового пространства 4 ГБ по умолчанию. Вы можете изменить параметр core_disk_request позже, после развертывания приложения.
inventory	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если все сервисы KUMA будут установлены внутри кластера, для параметра inventory установите значение /dev/null.
host_inventory	Нет	Путь к дополнительному файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Если вы выполняете первоначальное развертывание Kaspersky EDR Expert или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (/dev/null).
license	Нет	Путь к KUMA лицензионному ключу, находящемуся на устройстве администратора. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Вы можете загрузить лицензионный ключ или указать код активации при входе в OSMP после завершения развертывания.
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	Да	Имя устройства, которое используется в FQDN публичных служб Kaspersky EDR Expert. Имя устройства службы и доменное имя (значение параметра smp_domain) являются частью FQDN-службы. Значения параметров по умолчанию: • nwc_host – "console" • flow_host – "console" • hydra_host – "console" • login_host – "console" • ksc_host—"admsrv" • console_host – "console" • api_host – "api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	Да	Имя домена, которое используется в FQDN публичных служб Kaspersky EDR Expert. Значение параметра должно соответствовать требованиям назначения имен доменов до четвертого уровня. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной console_host равно console, а значение переменной smp_domain равно smp.local, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение console.smp.local.
pki_host_list	Да	Список имен устройств публичных служб Kaspersky EDR Expert, для которых требуется сформировать самоподписанный или пользовательский сертификат. Значение параметра должно быть списком имен устройств разделенных пробелами.

Имя параметра	Обязательная	Описание
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Kaspersky EDR Expert. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат. • `false` – использовать самоподписанные сертификаты (значение по умолчанию).
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, который используется для работы с общедоступными службами Kaspersky EDR Expert. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`. Значение параметра должно быть Linux-путем к файлу или содержимым файла в кодировке Base64. Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с соответствующими публичными службами Kaspersky EDR Expert: `<ksc_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<console_host>.<smp_domain>`, `<kuma_host>.<smp_domain>`, `<monitoring_host>.<smp_domain>`, и `<psql_host>.<smp_domain>`. Значения параметров должны быть Linux-путем к файлу или содержимым файла в кодировке Base64.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметр `intermediate_bundle`.

`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных). Измеряется в гигабайтах, указывается как "<объем>Gi". Требуемый объем свободного места на диске зависит от количества управляемых устройств и других параметров и может быть рассчитан. Значение по умолчанию – 30 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Измеряется в гигабайтах, указывается как "<объем>GB". Минимальное рекомендуемое значение и значение по умолчанию – 5 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.

`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Значение должно соответствовать следующим правилам:
		• Длина имени пользователя должна быть от 1 до 30 символов.
		• Имя пользователя может содержать следующие символы:
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (_ - .)
		• Имя пользователя должно начинаться с буквы.
		• Имя пользователя не должно содержать пробелов или символа "@".

`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
		Пароль должен соответствовать следующим правилам:
		• Пароль пользователя не может содержать менее 8 или более 256 символов.
		• Пароль должен содержать символы из указанных ниже групп:
		  • верхний регистр (A–Z);
		  • нижний регистр (a-z);
		  • числа (0–9);
		  • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

Имя параметра	Обязательная	Описание
`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение и значение по умолчанию – 40 ГБ. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. По умолчанию указано значение 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h"). Если вы не укажете этот параметр в конфигурационном файле, будет использоваться значение по умолчанию.
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.
`psql_tls_off`	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Kaspersky EDR Expert и СУБД по протоколу TLS. Если СУБД установлена за пределами кластера, шифрование TLS выключено по умолчанию. Если СУБД установлена внутри кластера, для **демонстрационного развертывания** необходимо выключить шифрование TLS (для параметра `psql_tls_off` установлено значение `true`). Возможные значения параметра: • `true` – трафик не шифруется (значение по умолчанию). • `false` – трафик шифруется.
`proxy_enabled`	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Kaspersky EDR Expert к интернету. Если устройство, на котором установлен Kaspersky EDR Expert, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Kaspersky EDR Expert (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. Возможные значения параметра: • `true` – использовать прокси-сервер. • `false` – не использовать прокси-сервер (значение по умолчанию).
`proxy_addresses`	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "`0.0.0.0 0.0.0.1 0.0.0.2`"). Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`proxy_port`	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`trace_level`	Нет	Уровень детализации файлов трассировки Сервера администрирования. Трассировка записывается во время работы Сервера администрирования. Значение по умолчанию – 0, трассировка не записывается. Возможные значения параметра: 0–5. Чем выше значение параметра, тем более подробная информация о трассировке записывается.
`ansible_extra_flags`	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • `-v` • `-vv` • `-vvv` • `-vvvv` По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.

Имя параметра	Обязательная	Описание
`incident_attachments_max_count_limit`	Нет	Количество файлов, которые вы можете прикрепить к инциденту. По умолчанию указано значение `100`.
`incident_attachments_max_size_limit`	Нет	Общий размер файлов, прикрепленных к инциденту. Измеряется в байтах. Единицы измерения не отображаются. По умолчанию указано значение `26214400`.
`ignore_precheck`	Нет	Параметр, указывающий, следует ли проверить аппаратное и программное обеспечение, а также конфигурацию сети узлов кластера Kubernetes на соответствие требованиям, необходимым для установки решения перед развертыванием. Возможные значения параметра: • `true` – пропустить предварительные проверки. • `false` – выполнить предварительные проверки (значение по умолчанию).
`airgap_mode`	Нет	Параметр, включающий или выключающий предварительную проверку и обновление кеша пакетов пакетным менеджером APT. Таким образом становится возможным развертывание Kaspersky EDR Expert в среде с физической изоляцией. Возможные значения параметра: • `true` – пропустить предварительную проверку и обновление кеша пакетов. • `false` – выполнить предварительную проверку и обновление кеша пакетов (значение по умолчанию).
`feature_gost_status`	Нет	Параметр, который указывает использовать ли рабочий процесс, созданный на основании ГОСТ Р 59712-2022, для управления инцидентами. Значение по умолчанию `false`. Возможные значения параметра: • `true` – рабочий процесс по ГОСТ используется. • `false` – рабочий процесс по ГОСТ не используется.
`grafana_smtp_host`	Нет	Адрес SMTP-сервера для Grafana, который используется для отправки уведомлений о событиях, связанных с работоспособностью кластера Kubernetes, по электронной почте. Укажите этот параметр в формате `<хост>:<порт>` – например, `localhost:25`.
`grafana_smtp_user`	Нет	Имя пользователя для аутентификации на SMTP-сервере.
`grafana_smtp_password`	Нет	Пароль для аутентификации на SMTP-сервере.
`grafana_smtp_bundle`	Нет	Файл, содержащий цепочку сертификатов X.509, которая используется для проверки TLS-подключения к SMTP-серверу.
`grafana_smtp_skip_verify`	Нет	Данный параметр указывает, следует ли пропускать проверку TLS-сертификата для SMTP-сервера. Возможные значения параметра: • `true` – пропустить проверку TLS-сертификата. • `false` – выполнять проверку TLS-сертификата (значение по умолчанию).
`grafana_smtp_from_address`	Нет	Электронный адрес отправителя, который будет отображаться в поле "От" при отправке уведомлений по электронной почте.
`grafana_smtp_from_name`	Нет	Отображаемое имя отправителя в уведомлениях по электронной почте.
`grafana_smtp_ehlo_identity`	Нет	Идентификатор, используемый в команде EHLO при подключении к SMTP-серверу.

Имя параметра	Обязательная	Описание
`grafana_starttls_policy`	Нет	Политика использования STARTTLS при подключении к SMTP-серверу. Возможные значения параметра: • `OpportunisticStartTLS` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования. • `MandatoryStartTLS` – требовать STARTTLS и завершаться с ошибкой, если SMTP-сервер не поддерживает STARTTLS. • `NoStartTLS` – не использовать STARTTLS и подключиться к SMPT-серверу без шифрования. • `empty` – использовать STARTTLS, если SMTP-сервер поддерживает его, а в противном случае подключиться к SMPT-серверу без шифрования (значение по умолчанию).
`grafana_smtp_enable_tracing`	Нет	Параметр, который указывает, следует ли включить ли трассировку SMTP-подключения для отладки отправки электронной почты. Возможные значения параметра: • `true` – включить трассировку SMTP-подключения. • `false` – отключить трассировку SMTP-подключения (значение по умолчанию).
`tokenhub_access_token`	Нет	Время жизни токена доступа. В конфигурационном файле установите значение параметра – "`<time in hours>h<time in minutes>m<time in seconds>s`". Например, "`1h10m`" или "`2h`". Минимальное значение – `5m`, а максимальное значение – `2h`. Значение по умолчанию – `1h`. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр `tokenhub_access_token` позже, после развертывания приложения.
`tokenhub_refresh_token`	Нет	Время жизни токена обновления, используемого для получения нового токена доступа. В конфигурационном файле установите значение параметра – "`<time in hours>h<time in minutes>m<time in seconds>s`". Например, "`24h`" или "`1240h30m`". Минимальное значение – `12m`, а максимальное значение – `4320h`. Значение по умолчанию – `24h`. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр `tokenhub_refresh_token` позже, после развертывания приложения.
`credentials_session_ttl`	Нет	Максимальное время простоя сеанса единого входа. В конфигурационном файле установите значение параметра – "`<time in hours>h<time in minutes>m<time in seconds>s`". Например, "`24h`" или "`1h30m`". Минимальное значение – `5m`, а максимальное значение – `96h`. Значение по умолчанию – `1h`. Если вы не укажете этот параметр в конфигурационном файле, будет использоваться это значение. Вы можете изменить параметр `credentials_session_ttl` позже, после развертывания приложения.

Пример конфигурационного файла для демонстрационного развертывания на одном узле

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky EDR will be deployed
nodes:
   # Node name.
  - desc: cdt-1
   # Node type.
   type: primary-worker
   # IP address of the node.
   host: 10.80.23.42
```

```
    access:
      ssh:
        # User name of the account.
        user: root
# Parameters for the Kaspersky EDR deployment
parameters:
  # IP address of the Kubernetes cluster gateway.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # Path to the SSH private key for connection to the primary worker node by KDT.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky EDR user account that will be created during the
  installation.
  - name: admin_password
    source:
      value: ""
  # The parameter indicating that Kaspersky EDR is installed on the target host with
  limited computing resources.
  - name: low_resources
    source:
      value: "true"
  # The number of disk volumes that are used to store the service data of Kaspersky EDR
  components and KDT. Для развертывания на одном узле установите для параметра значение
  "1".
  - name: default_class_replica_count
    source:
      value: "1"
  # Параметр, который указывает, следует ли запускать хранилище секретов в режиме High
  Availability (HA). Для развертывания на одном узле установите для параметра значение
  "false".
  - name: openbao_ha_mode
    source:
      value: "false"
  # Параметр, который указывает, следует ли запускать хранилище секретов в автономном
  режиме. Для развертывания на одном узле установите для параметра значение "true".
  - name: openbao_standalone
    source:
      value: "true"
  # Path to the KUMA inventory file that contains the installation parameters for
  deployment of the KUMA services.
  - name: inventory
    source:
      value: "/home/user/inventory.yml"
  # Путь к лицензионному ключу Ядра KUMA. Этот файл расположен на устройстве
  администратора.
  - name: license
    source:
      value: "/home/user/license.key"
  # Domain name. The service host name and domain name are parts of FQDNs of the
  Kaspersky EDR services.
  - name: smp_domain
    source:
      value: "smp.local"
  # List of host names of the Kaspersky EDR services for which a self-signed or custom
  certificate must be generated.
```

```
  - name: pki_host_list
    source:
      value: "admsrv api console kumamonitoring"
```

Начало работы

Следующие сценарии представляют собой пошаговые инструкции от первоначальной настройки Kaspersky EDR Expert до расследования инцидентов и поиска угроз.

Первоначальная настройка Kaspersky EDR Expert

Этот сценарий содержит действия по обязательной предварительной настройке и интеграции Kaspersky EDR Expert.

Предварительные требования

Перед тем как начать, убедитесь в следующем:

- У вас есть лицензионный ключ для Kaspersky EDR Expert и совместимых EPP-программ.
- Ваша инфраструктура соответствует требованиям к аппаратному и программному обеспечению.

Этапы

Основной сценарий первоначальной настройки состоит из следующих этапов:

1. **Активация**

   Активируйте по лицензии решение Kaspersky EDR Expert.

2. **Настройка мультитенантности**

   Если требуется, вы можете использовать возможности мультитенантности:

   1. Спланируйте и создайте требуемую иерархию тенантов.
   2. Создайте соответствующую иерархию Серверов администрирования в Open Single Management Platform.
   3. Привяжите тенанты к соответствующим Серверам администрирования.
   4. Создайте учетные записи для всех пользователей Kaspersky EDR Expert и назначьте роли.

3. **Добавление активов**

   Устройства в вашей инфраструктуре, которые необходимо защитить, представлены в Kaspersky EDR Expert как активы. Open Single Management Platform позволяет обнаруживать устройства в вашей сети и управлять их защитой. Вы также сможете добавлять активы вручную или импортировать их из других источников на этапе 8.

   Учетные записи пользователей также представлены как активы в Kaspersky EDR Expert. Убедитесь что интеграция с Active Directory на этапе 9 настроена, чтобы включить отображение затронутых учетных записей пользователей в связанных событиях, алертах и инцидентах.

4. **Добавление пользователей и назначение ролей**

   Назначьте роли учетным записям пользователей, чтобы определить их права доступа к различным функциям Kaspersky EDR Expert в зависимости от их задач.

5. **Подключение к SMTP-серверу**

   Настройте подключение к SMTP-серверу для получения уведомлений по электронной почте о событиях, возникающих в Kaspersky EDR Expert.

6. **Настройка источников событий, хранения и корреляции**

   Укажите, откуда должны быть получены события, а также как они должны храниться и обрабатываться:

   1. Настройте интеграцию Kaspersky Unified Monitoring and Analysis Platform и Kaspersky Security Center.
   2. Импортируйте активы из Kaspersky Security Center.
   3. Добавьте активы вручную или импортируйте их из других источников (необязательно).
   4. Настройте источники событий, чтобы указать, откуда вы хотите получать события.
   5. Создайте хранилище для событий.
   6. Создайте коллекторы для приема, обработки (нормализации) и передачи событий.
   7. Создайте корреляторы для первоначального анализа нормализованных событий и их дальнейшей обработки.

      При создании коррелятора вы можете создать правила корреляции, которые определяют правила обработки и реагирования на события, а также импортировать ранее сохраненные правила корреляции или использовать готовый набор правил корреляции, входящий в состав решения Kaspersky EDR Expert. После создания коррелятора вы можете связать правила корреляции с коррелятором, если это необходимо.

      > Рекомендуется настроить исключения на этом этапе, чтобы избежать ложных срабатываний и нерелевантных данных.

7. **Настройка интеграций**

   Настройте интеграцию Kaspersky EDR Expert с Active Directory и другими решениями "Лаборатории Касперского", чтобы расширить его возможности и обогатить данные, доступные для расследования инцидентов.

   1. Интеграция с Active Directory (рекомендуется).
   2. Интеграция с Kaspersky CyberTrace (необязательная интеграция; требуется лицензия).

3. Интеграция с Kaspersky TIP (необязательная интеграция; требуется лицензия) или Kaspersky Open TIP.

4. Интеграция с Kaspersky Managed Detection and Response (необязательная интеграция; необходима лицензия).

8. **Настройка обновлений**

   Создайте задачу Загрузка обновлений в хранилище Сервера администрирования.

9. **Проверка корректности конфигурации**

   Используйте тестовый файл EICAR на одном из активов. Если первоначальная настройка была выполнена правильно и были настроены необходимые правила корреляции, это событие вызовет создание алерта в списке алертов.

После завершения первоначальной настройки события от защищаемых активов будут получены и обработаны Kaspersky EDR Expert, а при срабатывании правила корреляции будет создан алерт.

Проверка настройки Kaspersky EDR Expert

Вы можете использовать тестовый "вирус" EICAR на одном из активов, чтобы убедиться, что Kaspersky EDR Expert правильно развернут и настроен. Если первоначальная настройка была выполнена правильно и были настроены необходимые правила корреляции, соответствующее событие вызовет создание алерта в списке алертов.

Чтобы проверить настройку Kaspersky EDR Expert:

1. Создайте коррелятор в Консоли OSMP в разделе KUMA.

   При создании коррелятора не указывайте параметры в разделе **Корреляция**.

2. Импортируйте правила корреляции из пакета SOC Content, чтобы получить предустановленные правила корреляции, используемые для обнаружения тестового "вируса" EICAR.

3. Укажите правило корреляции для созданного коррелятора.

   Вы можете указать правило корреляции одним из следующих способов:

   - Свяжите предустановленное правило корреляции с созданным коррелятором:

     a. Перейдите в раздел **Ресурсы**, нажмите на **Правила корреляции** и выберите тенант, к которому будет применяться правило корреляции.

     b. В списке предустановленных правил корреляции выберите правило **R077_02_KSC.Malware detected**, чтобы обнаруживать события Kaspersky Security Center.

     c. Нажмите на **Связать с коррелятором** и выберите созданный коррелятор, чтобы связать выбранное правило корреляции с коррелятором.

- Создайте правило корреляции с предустановленными фильтрами вручную:

  a. Откройте параметры созданного коррелятора, перейдите в раздел **Корреляция** и нажмите на кнопку **Добавить**.

  b. В окне **Создание правила корреляции** на вкладке **Общие** задайте следующие параметры, так же как и другие параметры:

     - **Вид**: простой.

     - **Наследуемые поля**: DestinationAddress, DestinationHostName, DestinationAccountID, DestinationAssetID, DestinationNtDomain, DestinationProcessName, DestinationUserName, DestinationUserID, SourceAccountID, SourceUserName.

  c. Перейдите в раздел **Селекторы** → **Параметры** и укажите выражение для фильтрации необходимых событий:

     - В режиме конструктора добавьте фильтры событий **KSC**, **Обнаружен вирус приложением KSC** и **Базовые события** с помощью оператора AND.

     - Также вы можете указать это выражение в режиме исходного кода следующим образом:

       ```
       filter='b308fc22-fa79-4324-8fc6-291d94ef2999'
       AND filter='a1bf2e45-75f4-45c1-920d-55f5e1b8843f'
       AND filter='1ffa756c-e8d9-466a-a44b-ed8007ca80ca'
       ```

  d. В разделе **Действия** в параметрах правила корреляции установите только флажок **В дальнейшую обработку** (флажки **В коррелятор** и **Не создавать алерт** должны быть сняты). В этом случае при обнаружении тестового "вируса" EICAR будет создано событие корреляции и в списке алертов Kaspersky EDR Expert будет создан алерт.

  e. Нажмите на кнопку **Создать**, чтобы сохранить параметры правила корреляции, связанные с коррелятором.

4. Создайте и настройте в разделе KUMA Консоли OSMP коллектор для получения информации о событиях Сервера администрирования из базы данных MS SQL.

   Также вы можете использовать предустановленный коллектор [OOTB] KSC SQL.

5. В разделе параметров коллектора **Маршрутизация** установите **Тип коррелятора** и укажите созданный коррелятор в поле **URL**, чтобы пересылать ему обработанные события.

6. Установите Агент администрирования и приложение защиты конечных точек (например, Kaspersky Endpoint Security) на актив в сети вашей организации. Убедитесь, что актив подключен к Серверу администрирования.

7. Поместите тестовый файл EICAR на актив, а затем обнаружьте тестовый "вирус" с помощью приложения защиты конечных точек.

После этого Сервер администрирования получит уведомление о событии на активе. Это событие будет перенаправлено в компонент KUMA, преобразовано в событие корреляции, после чего в Kaspersky EDR Expert будет создан алерт в списке алертов. Если алерт создан, значит Kaspersky EDR Expert работает правильно.

Использование функций мониторинга, обнаружения и поиска угроз

После установки и настройки Kaspersky EDR Expert вы можете использовать функции Kaspersky EDR Expert для мониторинга безопасности вашей инфраструктуры, расследования инцидентов безопасности, автоматизации рабочих процессов и автоматического поиска угроз:

- **Использование панели мониторинга и настройка виджетов**

  Вкладка **Обнаружение и реагирование** в панели мониторинга может содержать виджеты, которые отображают информацию о зарегистрированных алертах и инцидентах, а также действиях по реагированию на них. Вы можете использовать и настраивать предварительно настроенные макеты виджетов для своей панели мониторинга или создавать макеты и виджеты.

  Open Single Management Platform также предоставляет различные инструменты для мониторинга безопасности и создания отчетов.

- **Использование отчетов**

  Вы можете настроить формирование отчетов в Kaspersky Unified Monitoring and Analysis Platform для получения необходимых сводных данных по указанному расписанию.

- **Использование поиска угроз**

  Вы можете использовать инструменты поиска угроз для анализа событий и поиска угроз и уязвимостей, которые не были обнаружены автоматически. Поиск угроз можно использовать как для расследования инцидентов и алертов, так и для предупреждающего поиска угроз.

- **Использование плейбуков**

  Вы можете использовать плейбуки для автоматизации действий по реагированию на алерты и инциденты в соответствии с заданным алгоритмом. Существует ряд предустановленных плейбуков, которые вы можете запускать в различных режимах работы. Вы можете создавать пользовательские плейбуки.

Пример расследования инцидента с помощью Kaspersky EDR Expert

Этот сценарий представляет собой пример рабочего процесса расследования инцидента.

Расследование инцидента состоит из следующих этапов:

1. **Назначение алерта пользователю**

   Вы можете назначить алерт себе или другому пользователю.

2. **Проверка совпадения сработавшего правила корреляции с данными событий алерта**

   Просмотрите информацию об алерте и убедитесь, что данные о событии алерта соответствуют сработавшему правилу корреляции. Если алерт является ложным срабатыванием, измените правило корреляции.

3. **Анализ информации об алерте**

   Проанализируйте информацию об алерте, чтобы определить, какие данные требуются для дальнейшего анализа алерта.

4. **Обогащение вручную**

   Запустите доступные решения для дополнительного обогащения события (например, Kaspersky TIP).

5. **Проверка ложного срабатывания**

   Убедитесь, что действие, запустившее правило корреляции, является аномальным для ИТ-инфраструктуры организации.

6. **Создание инцидента**

   Если шаги с 3 по 5 показывают, что алерт требует расследования, вы можете создать инцидент или связать алерт с существующим инцидентом.

   Вы также можете объединить инциденты.

7. **Управление инцидентами.**

   Вы можете управлять инцидентами, изменяя статусы инцидентов и их приоритеты, а также назначая инциденты другим аналитикам.

   Можно управлять SLA инцидентов, типами инцидентов и рабочими процессами. Также вы можете отслеживать трудозатраты на работу, связанную с инцидентом.

8. **Расследование**

   Этот шаг включает в себя просмотр информации об активах, учетных записях пользователей и алертах, связанных с инцидентом. Вы можете использовать граф расследования и инструменты поиска угроз, чтобы получить дополнительную информацию.

9. **Поиск связанных активов**

   Вы можете просмотреть алерты, которые возникли на активах, связанных с инцидентом.

10. **Поиск связанных событий**

    Вы можете расширить область расследования, выполнив поиск событий связанных алертов.

11. **Просмотр истории инцидента**

    Вы можете просмотреть журнал изменений инцидента и историю реагирования.

12. **Добавление комментариев**

    Вы можете оставлять комментарии с информацией, необходимой для расследования инцидента.

13. **Действие по реагированию**

    Вы можете выполнять действия по реагированию вручную.

14. **Реагирование с помощью плейбуков**

    Вы можете выполнить действие по реагированию на инцидент, запустив плейбук вручную.

15. **Закрытие инцидента**

    После принятия мер по удалению следов присутствия злоумышленника в ИТ-инфраструктуре организации можно закрыть инцидент.

Обновление Kaspersky EDR Expert с версии 8.2 до версии 8.3

Чтобы обновить решение Kaspersky EDR Expert, выполните следующие действия.

1. **Переустановите Sandbox.**

   Поскольку обновления для компонента Sandbox недоступны, необходимо установить новую версию Sandbox и интегрировать ее с Kaspersky EDR Expert.

   При установке на VMware ESXi необходимо настроить VMware ESXi в соответствии с рекомендациями в разделе Расчеты для компонента Sandbox.

   После установки укажите максимальное количество виртуальных машин, которые могут работать одновременно. По умолчанию задано значение 48.

2. **Обновите компоненты Kaspersky EDR Expert.**

   Вы можете обновить Kaspersky EDR Expert с версии 8.2 до 8.3 с помощью KDT. KDT обновляет кластер Kubernetes и компоненты Kaspersky EDR Expert. При обновлении вам не нужно заполнять конфигурационный файл, так как используются параметры установки, указанные во время развертывания. Шаги обновления Kaspersky EDR Expert с предыдущей версии не зависят от выбранного варианта развертывания.

   Чтобы обновить компоненты Kaspersky EDR Expert:

   1. Скачайте и распакуйте дистрибутив Kaspersky EDR Expert версии 8.3.

   2. Ознакомьтесь с Лицензионным соглашением KDT, находящимся в дистрибутиве с компонентами Kaspersky EDR Expert.

      Когда вы начинаете использовать KDT, вы принимаете условия Лицензионного соглашения KDT.

      Вы можете ознакомиться с Лицензионным соглашением KDT после обновления Kaspersky EDR Expert. Файл `license_kdt.txt` находится в директории `~/kaspersky_eula` пользователя, который запускает обновление Kaspersky EDR Expert.

   3. Выполните следующую команду для обновления Kaspersky EDR Expert и компонента Bootstrap:

      ```
      ./kdt apply -k <полный_путь_к_архиву_обновлений_XDR>
      ```

      Чтобы начать обновление Kaspersky EDR Expert, примите условия Лицензионного соглашения и Политики конфиденциальности.

      Вы можете установить Kaspersky EDR Expert без запроса на ознакомление с условиями Лицензионного соглашения и Политикой конфиденциальности OSMP, если вы используете флаг `--accept-eula`. В этом случае вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности OSMP перед обновлением Kaspersky EDR Expert. Файлы находятся в дистрибутиве с компонентами Kaspersky EDR Expert. Используя флаг `--accept-eula`, вы подтверждаете, что полностью прочитали, поняли и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

      Если вы хотите прочитать и принять условия Лицензионного соглашения и Политики конфиденциальности во время обновления, не используйте флаг `--accept-eula`.

   4. Если вы не использовали флаг `--accept-eula` на предыдущем шаге, прочтите Лицензионное соглашение и Политику конфиденциальности OSMP. Текст отображается в окне командной строки.

Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

- Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

  Введите `n`, если вы не принимаете условия Лицензионного соглашения.

- Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны) в соответствии с Политикой конфиденциальности.

  Введите `n`, если вы не принимаете условия Политики конфиденциальности.

Если вы не принимаете условия Лицензионного соглашения и Политики конфиденциальности, приложение Kaspersky EDR Expert не будет обновлено.

5. Скачайте пакет `chrome_full.tar.gz`, поместите его в директорию `/root/xdr/kdt/bin/` и выполните следующую команду:

```
./kdt invoke kuma --action=enableReporting --if reporting_archive=chrome_full.tar.gz
```

Эта команда обеспечивает корректное создание отчетов в форматах PDF и HTML.

6. Импортируйте коллектор [OOTB] Kaspersky OSMP (в предыдущих версиях назывался **[OOTB] Kaspersky OSMP audit**), чтобы гарантировать получение событий аудита от компонентов OSMP. В зависимости от конфигурации хранилища выполните следующие действия:

- Хранилище по умолчанию в Kaspersky EDR Expert 8.2 → хранилище по умолчанию в Kaspersky EDR Expert 8.3.

  Если хранилище по умолчанию **[OOTB] OSMP Storage** было настроено в коллекторе **[OOTB] Kaspersky OSMP** в OSMP 2.2 и будет использоваться после обновления до версии OSMP 2.3, перейдите в раздел **Активные сервисы** и перезапустите сервис коллектора [OOTB] Kaspersky OSMP. Никаких дополнительных действий не требуется.

- Хранилище по умолчанию в Kaspersky EDR Expert 8.2 → пользовательское хранилище в Kaspersky EDR Expert 8.3.

  Если хранилище по умолчанию **[OOTB] OSMP Storage** было настроено в коллекторе **[OOTB] Kaspersky OSMP** в Kaspersky EDR Expert 8.2 и вы решили переключиться на другое хранилище после обновления до версии Kaspersky EDR Expert 8.3:

a. Убедитесь, что пространство **osmp_technical_events** создано в другом хранилище.

b. Убедитесь, что в другом хранилище настроены те же теги, что и в хранилище по умолчанию **[OOTB] OSMP Storage**.

c. Перейдите в раздел **Активные сервисы** и перезапустите сервис коллектора [OOTB] Kaspersky OSMP.

Пользовательское хранилище в Kaspersky EDR Expert 8.2 → пользовательское хранилище в Kaspersky EDR Expert 8.3.

- Если вы настроили другое хранилище для коллектора **[OOTB] Kaspersky OSMP** в OSMP 2.2 и это хранилище используется после обновления до версии OSMP 2.3:

a. Убедитесь, что пространство **osmp_technical_events** создано в другом хранилище.

b. Убедитесь, что в другом хранилище настроены те же теги, что и в хранилище по умолчанию **[OOTB] OSMP Storage**.

c. Перейдите в раздел **Активные сервисы** и перезапустите сервис коллектора [OOTB] Kaspersky OSMP.

7. Измените файл ресурсов коллектора:

a. Скопируйте идентификатор ресурса коллектора. Перейдите в раздел **Активные сервисы** и в списке сервисов нажмите на название коллектора **[OOTB] Kaspersky OSMP**, а затем скопируйте идентификатор ресурса коллектора одним из следующих способов:

- В панели параметров коллектора скопируйте значение идентификатора ресурса из URL в вашем браузере.

- Скопируйте идентификатор ресурса коллектора из терминала.

  - Выполните следующую команду на одном из управляющих узлов кластера Kubernetes:

```
k0s kubectl get collector -n kuma   -o custom-
columns=SERVICE_NAME:.metadata.name,RESOURCE_ID:.spec.clusterId
```

  - Скопируйте идентификатор ресурса коллектора из таблицы:

```
SERVICE_NAME   RESOURCE_ID
<collector service ID>   <collector resource ID>
```

Не используйте кнопку **Копировать идентификатор** в контекстном меню коллектора, так как она копирует идентификатор сервиса коллектора. Вместо этого вам нужно использовать идентификатор ресурса коллектора.

a. Выполните следующую команду, используя скопированный идентификатор ресурса коллектора, чтобы открыть файл ресурсов коллектора в редакторе:

```
k0s kubectl edit service/collector-cluster-<идентификатор ресурса коллектора> -n kuma
```

Файл ресурсов коллектора открыт в редакторе.

b. В секции labels добавьте запись `kuma.kaspersky.com/sd: osmp-logs` и сохраните файл ресурсов коллектора.

KDT выполняет обновление и отображает ход обновления в консоли. Дождитесь завершения обновления. Решение Kaspersky EDR Expert будет обновлено с версии 8.2 до версии 8.3.

3. **Установите веб-плагин Kaspersky Endpoint Security.**

   Необходимые веб-плагины входят в состав комплекта поставки.

   Веб-плагины Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux уже включены в пакет Kaspersky EDR Expert, поэтому дополнительно устанавливать их не требуется.

   Чтобы установить веб-плагин Kaspersky Endpoint Security для Mac, используйте утилиту KDT.

4. **Обновите приложения EPP**

   Обновите приложения EPP до последних совместимых версий. Инструкция по обновлению приложения приведена в документации Kaspersky Endpoint Security:

   - Обновление Kaspersky Endpoint Security для Windows
   - Обновление Kaspersky Endpoint Security для Linux
   - Обновление Kaspersky Endpoint Security для Mac

   Также может потребоваться информация о миграции с конфигурации [KES+KEA] на конфигурацию [KES+встроенный агент].

Перенос данных в Kaspersky EDR Expert

В этом разделе описывается перенос данных в Kaspersky EDR Expert 8.3 из Kaspersky Security Center Windows и KEDR 7.1.

О переносе данных из Kaspersky Security Center Windows

Следуя этому сценарию, вы можете передать структуру группы администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky EDR Expert.

Ограничения:

- Перенос данных возможен только с Kaspersky Security Center 15.1 Windows в Kaspersky EDR Expert, начиная с версии 8.0.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Этапы

Сценарий переноса данных состоит из следующих этапов:

1. **Выберите способ переноса данных**

   Вы переносите данные в Kaspersky EDR Expert с помощью мастера переноса данных. Шаги мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky EDR Expert в иерархию:

   - Перенос данных с использованием иерархии Серверов администрирования

     Выберите этот вариант, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky EDR Expert. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Консоли OSMP. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого перед началом переноса данных создайте иерархию.

     При подключении подчиненных Серверов администрирования к Kaspersky EDR Expert, выключите фоновую интеграцию для Web Console, которые управляют ими.

     Чтобы отключить фоновую интеграцию:

     1. Войдите в Web Console Сервера администрирования.
     2. В главном окне приложения перейдите в раздел **Параметры** → **Интеграция**.
     3. В разделе **Фоновое соединение** отключите параметр **Фоновое соединение для интеграции Включено**.

- Перенос данных с помощью файла экспорта (ZIP-архив)

  Выберите этот вариант, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky EDR Expert не организованы в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров Консоли, одного экземпляра Kaspersky Security Center Windows и другого Консоли OSMP. В этом случае вы используете файл экспорта, который вы создали и загрузили при экспорте из Kaspersky Security Center Windows, и импортируете этот файл в Kaspersky EDR Expert.

2. **Экспорт данных из Kaspersky Security Center Windows**

   Откройте Kaspersky Security Center Windows и запустите мастер переноса данных.

3. **Импорт данных в Kaspersky EDR Expert**

   Продолжите работу мастера передачи данных, чтобы импортировать экспортированные данные в Kaspersky EDR Expert.

   Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера передачи данных после перехода на Kaspersky EDR Expert.

4. **Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky EDR Expert вручную (необязательный шаг)**

   Вы также можете перенести объекты и параметры, которые невозможно передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

   - Настроить глобальные задачи Сервера администрирования.
   - Настроить параметры политики Агента администрирования.
   - Создать инсталляционные пакеты приложений.
   - Создать виртуальные Серверы администрирования.
   - Назначить и настроить точки распространения.
   - Создать правила перемещения устройств.
   - Настроить правила автоматического назначения тегов устройствам.
   - Создать категории приложений.

5. **Переместить импортированные управляемые устройства под управление Kaspersky EDR Expert**

   Для завершения переноса данных переместите импортированные управляемые устройства под управление Kaspersky EDR Expert. Вы можете воспользоваться одним из следующих способов:

   - С помощью групповой задачи Kaspersky Security Center

     Используйте задачу Сменить Сервер администрирования, чтобы сменить Сервер администрирования на другой для конкретных клиентских устройств.

   - С помощью утилиты klmover.

     Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.

- С помощью установки или переустановки Агента администрирования на управляемые устройства.

  Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Используя инсталляционный пакет, установите Агент администрирования на импортированные управляемые устройства с помощью задачи удаленной установки.

  Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

6. **Обновите Агент администрирования до последней версии.**

   Рекомендуется обновить Агент администрирования до той же версии, что и Консоль OSMP.

7. **Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.**

   На Сервере администрирования Kaspersky EDR Expert откройте список управляемых устройств (**Управление активами** → **Активы (Устройства)**) и проверьте значения в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

Другие способы переноса данных

Помимо мастера переноса данных, вы также можете переносить определенные задачи и политики:

- Экспортируйте задачи из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky EDR Expert.
- Экспортируйте политики из Kaspersky Security Center Windows, а затем импортируйте эти политики в Kaspersky EDR Expert. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, которая включает управляемые устройства и другие объекты группы из Kaspersky Security Center Windows в Kaspersky EDR Expert, необходимо, чтобы вы сначала выбрали данные для экспорта и создали файл экспорта. Файл экспорта содержит информацию обо всех групповых объектах, которые вы хотите перенести. Файл экспорта будет использован для последующего импорта в Kaspersky EDR Expert.

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

Перед тем, как начать экспорт, ознакомьтесь с общей информацией о переносе данных в Kaspersky EDR Expert. Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Kaspersky EDR Expert.

Чтобы экспортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky EDR Expert в иерархию, выполните одно из следующих действий:

   - Если Серверы организованы в иерархию, откройте Консоль OSMP и переключитесь на Сервер Kaspersky Security Center Windows.

   - Если Серверы не организованы в иерархию, откройте Kaspersky Security Center Web Console, подключенную к Kaspersky Security Center Windows.

2. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

3. Выберите **Перенос данных в Kaspersky Security Center Linux или Open Single Management Platform**, чтобы запустить мастер, и следуйте его шагам.

4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.

5. Выберите управляемые приложения, задачи и политики которых будут экспортированы. Выбирайте только те приложения, которые поддерживаются Kaspersky EDR Expert. Объекты неподдерживаемых приложений все равно будут экспортированы, но не будут работать.

6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Группировать объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории приложений.

Файл экспорта (ZIP-архив) создан. В зависимости от того, выполняете ли вы перенос данных с поддержкой иерархии Сервера администрирования, файл экспорта сохраняется следующим образом:

- Если Серверы организованы в иерархию, файл экспорта сохраняется во временной папке на Сервере OSMP.

- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

При переносе данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта. При переносе данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky EDR Expert.

Импорт файла экспорта в Kaspersky EDR Expert

Чтобы перенести информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows, вам необходимо импортировать ее в Kaspersky EDR Expert.

Чтобы импортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky EDR Expert в иерархию, выполните одно из следующих действий:

   - Если Серверы организованы в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта в этом мастере (см. шаг 2 этой инструкции).

   - Если Серверы не организованы в иерархию:

     a. Откройте консоль OSMP.

     b. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

     c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows. Начнется загрузка файла экспорта.

2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если Серверы не организованы в иерархию, вы можете указать другой файл экспорта, перейдя по ссылке **Изменить** и выбрав нужный файл.

3. Отображается вся иерархия групп администрирования Kaspersky EDR Expert.

   Установите флажок рядом с целевой группой администрирования, в которой необходимо восстановить объекты экспортированной группы администрирования (управляемые устройства, политики, задачи и другие объекты группы).

4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится.

5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

> Если в перенесенной задаче указаны данные учетной записи, под которой она запускается, вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

Если импорт завершился с ошибкой, вы можете выполнить одно из следующих действий:

- Для переноса данных с поддержкой иерархии Сервера администрирования вы можете импортировать файл экспорта еще раз. В этом случае вам необходимо выбрать группу администрирования, как описано на шаге 3.

- Для переноса данных без поддержки иерархии Сервера администрирования вы можете запустить мастер переноса данных, чтобы выбрать другой файл экспорта, а затем импортировать его снова.

Вы можете проверить, были ли объекты группы, входящие в область экспорта, успешно импортированы в Kaspersky EDR Expert. Для этого перейдите в раздел **Управление активами** и убедитесь, что импортированные объекты отображаются в соответствующих подразделах.

Обратите внимание, что импортированные управляемые устройства отображаются в подразделе **Управляемые устройства**, но они не видны в сети, и Агент администрирования не установлен и не запущен на них (значение *Нет* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**).

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky EDR Expert, как описано на этапе 5 раздела Перенос данных в Kaspersky EDR Expert.

Переключение управляемых устройств под управление Kaspersky EDR Expert

После успешного импорта информации об управляемых устройствах, объектах и их параметрах в Kaspersky EDR Expert для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky EDR Expert.

Вы можете переместить управляемые устройства под управление Kaspersky EDR Expert одним из следующих способов:

- Используя утилиту klmover.
- Используя задачу *Смена Сервера* администрирования.
- Установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки.

Чтобы переключить управляемые устройства под управление Kaspersky EDR Expert, установив Агент администрирования:

1. Удалите Агент администрирования на импортированных управляемых устройствах, которые будут переключены под управление Kaspersky EDR Expert.
2. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.
3. Перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования.

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый.

   Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.
4. На вкладке **Параметры** выберите раздел **Подключение**. Укажите параметры подключения Сервера администрирования Kaspersky EDR Expert.
5. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования.

   Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения. Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точек распространения**.
6. Запустите задачу удаленной установки приложения.

После успешного завершения задачи удаленной установки перейдите на Сервер администрирования Kaspersky EDR Expert и убедитесь, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

О переносе данных из KEDR 7.1

Прямой перенос данных из Kaspersky EDR Expert 7.1 в 8.3 не поддерживается, так как версия 8.3 имеет лишь незначительные функциональные отличия от версии 8.1.

Чтобы перенести данные из Kaspersky EDR Expert 7.1 в Kaspersky EDR Expert 8.3, выполните следующие действия:

1. Установите Kaspersky EDR Expert 8.1.
2. Выполните перенос данных из Kaspersky EDR Expert 7.1 в Kaspersky EDR Expert 8.1, как описано в справке Kaspersky EDR Expert 8.1.

   Для переноса данных необходимо использовать пакет cnab gateway-migration, находящийся в транспортном архиве. Устанавливать и запускать cnab gateway-migration необходимо под учетной записью пользователя, который устанавливал Kaspersky EDR Expert.
3. Обновите Kaspersky EDR Expert с версии 8.1 до версии 8.3.

Настройка компонента SIEM и работа с ним

В этой главе представлена информация об установке и настройке SIEM-системы KUMA.

Службы KUMA

Службы – это основные компоненты KUMA, с помощью которых система осуществляет работу с событиями: службы позволяют получить события из источников, чтобы в дальнейшем привести их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть службы создается внутри Консоли KUMA на основе набора ресурсов для служб.
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть службы может состоять из нескольких экземпляров: например, службы одного и того же хранилища могут быть установлены сразу на нескольких устройствах.

  В серверной части службы KUMA располагаются в директории `/opt/kaspersky/kuma`.

  При установке KUMA в режиме высокой доступности в кластере устанавливается только Ядро KUMA. Коллекторы, корреляторы и хранилища размещаются на устройствах вне кластера Kubernetes.

Между собой части служб соединены с помощью идентификатора служб.

Типы сервисов:

- Коллекторы используются для получения событий и преобразования их в формат KUMA.
- Корреляторы используются для анализа событий и поиска закономерностей.
- Хранилища используются для хранения событий.

В Консоли KUMA сервисы отображаются в разделе **Ресурсы** → **Активные сервисы** в виде таблицы. Таблицу сервисов можно обновлять с помощью кнопки **Обновить** и сортировать по столбцам, нажимая на активные заголовки.

Максимальный размер таблицы не ограничен. Если вы хотите выбрать все сервисы, прокрутите таблицу до конца и установите флажок **Выбрать все**, таким образом все доступные в таблице сервисы будут выбраны.

Столбцы таблицы:

- **Статус** – статус сервиса:
  - Зеленый – сервис работает.
  - Красный – сервис не работает.
  - Желтый – сервис работает, но есть ошибки или алерты от VictoriaMetrics. Сообщение об ошибке можно просмотреть, наведя курсор мыши на статус.

- Фиолетовый – этот статус применяется к работающим сервисам, у которых изменился конфигурационный файл в базе данных и при этом отсутствуют другие ошибки. Если у сервиса некорректный конфигурационный файл и есть ошибки, например от VictoriaMetrics, статус сервиса будет желтым.

- Серый – если в удаленном тенанте была работающий сервис, который продолжает работать, на странице **Активные сервисы** он будет отображаться с серым статусом. Сервисы в сером статусе остаются, чтобы вы могли скопировать идентификатор и удалить сервисы на серверах. Удалить сервисы с серым статусом может только Главный администратор. Когда тенант удаляется, его службы назначаются главному тенанту.

- **Тип** – вид сервиса: **коллектор**, **коррелятор**, **хранилище**.

- **Название** – название сервиса. При нажатии на название сервиса открываются его параметры.

- **Версия** – версия сервиса.

- **Тенант** – название тенанта, которому принадлежит сервис.

- **Полное доменное имя** – доменное имя сервера, на котором установлен сервис.

- **IP-адрес** – IP-адрес сервера, на котором установлен сервис.

- **Порт API** – номер порта для внутренних коммуникаций.

- **Время работы** – как долго работает сервис.

- **Создан** – дата и время создания сервиса.

В таблице предусмотрена сортировка данных по возрастанию и убыванию, а также по параметру **Статус**. Вы можете отсортировать активные сервисы, вызвав контекстное меню правой кнопкой мыши и выбрав один или несколько статусов.

С помощью кнопок в верхней части окна **Службы** можно выполнить следующие групповые действия:

- Добавить сервис.

  Вы можете создавать новые сервисы на основе существующих наборов ресурсов для сервисов. Не рекомендуется создавать сервисы вне основного тенанта без предварительного внимательного планирования межтенантных взаимодействий различных сервисов и пользователей.

- Обновить.

  Вы можете обновить список активных сервисов.

- Обновить параметры.

- Перезапустить.

Для действий с отдельными сервисами воспользуйтесь контекстным меню, которое вы можете вызвать нажатием правой кнопки мыши. Доступны следующие действия:

- Сбросить сертификат.

- Удалить

- Скачать журнал.

  Если вы хотите получать детализированные данные, настройте в параметрах сервиса режим Отладка.

- Скопировать идентификатор сервиса

  Идентификатор понадобится вам для установки, перезапуска, остановки или удаления сервиса.

- Перейти к событиям.

- Перейти к активным листам.

- Перейти к контекстным таблицам.

- Перейти к партициям.

Чтобы изменить сервис, выберите его в разделе **Ресурсы** → **Активные сервисы**. Откроется окно с набором ресурсов, на основе которых был создан сервис. Вы можете изменить параметры набора ресурсов и сохранить изменения. Чтобы применить сохраненные изменения, перезапустите сервис.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. Если требуется изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Инструменты сервисов

В этом разделе описываются инструменты по работе с сервисами, доступные в OSMP в разделе **Ресурсы и сервисы** → **Активные сервисы**.

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса – расположенных внутри OSMP и установленных в сетевой инфраструктуре – в единый комплекс. Идентификатор присваивается сервису при его создании в OSMP, а затем используется при установке сервиса на сервер.

Чтобы получить идентификатор сервиса:

1. Войдите в Консоль OSMP и откройте раздел **Ресурсы и сервисы** → **Активные сервисы**.

2. Установите флажок рядом с сервисом, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

   Идентификатор сервиса помещен в буфер обмена. Его можно использовать, например, для установки сервиса на сервере.

Остановка, запуск и проверка статуса сервиса

В ходе работы с OSMP может возникнуть необходимость в следующих операциях:

- Временно остановить сервис. Например, в процессе восстановления Ядра из резервной копии или если вы хотите отредактировать параметры сервиса, связанные с операционной системой.
- Запустить сервис.
- Проверить статус сервиса.

В таблице ниже перечислены команды, которые могут быть полезны при управлении OSMP.

Команды остановки, запуска и проверки статуса сервиса

Сервис	Остановить сервис	Запустить сервис	Проверить статус сервиса
Ядро	`sudo systemctl stop kuma-core.service`	`sudo systemctl start kuma-core.service`	`sudo systemctl status kuma-core.service`
Сервисы с идентификатором: • collector • correlator • storage	`sudo systemctl stop kuma-<collector/correlator/storage>-< идентификатор сервиса >.service`	`sudo systemctl start kuma-<collector/correlator/storage>-< идентификатор сервиса >.service`	`sudo systemctl status kuma-<collector/correlator/storage>< идентификатор сервиса >.service`
Сервисы без идентификатора: • kuma-grafana.service • kuma-mongodb.service • kuma-victoria-metrics.service • kuma-vmalert.service	`sudo systemctl stop kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl start kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl status kuma-<grafana/victoria-metrics/vmalert>.service`

Перезапуск службы

Чтобы перезапустить сервис:

1. Войдите в Консоль OSMP и откройте раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом со службой и выберите нужный параметр:
   - **Обновить параметры** – обновить конфигурацию работающей службы, не останавливая его. Например, так можно изменить настройки сопоставления полей или параметры точки назначения.
   - **Перезапустить** – остановить службу и запустить ее снова. Этот параметр используется для изменения таких параметров, как порт или тип коннектора.
   - **Сбросить сертификат** – удалить сертификаты, используемые службы для внутренней связи. Этот параметр невозможно использовать для обновления сертификата Ядра KUMA. Чтобы обновить сертификаты Ядра KUMA, их следует перевыпустить.

Удаление службы

Перед удалением сервиса получите его идентификатор. Идентификатор потребуется, чтобы удалить сервис с сервера.

Чтобы удалить сервис в OSMP:

1. Войдите в Консоль OSMP и откройте раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с нужном сервисом и нажмите **Удалить**.

   Откроется окно подтверждения.
3. Нажмите на кнопку **OK**.

Сервис удален из OSMP.

Чтобы удалить сервис с сервера, выполните команду:

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id < идентификатор службы >
--uninstall
```

Сервис удален с сервера.

Просмотр таблицы активных запросов

Под учетной записью с правами Главного администратора вы можете просмотреть запросы других пользователей и ресурсов OSMP, которые выполняются в этот момент.

Чтобы просмотреть таблицу активных запросов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажки рядом с нужными хранилищами.
3. В панели инструментов или в меню (⋮) нажмите **Активные запросы**.

   Откроется окно с таблицей **Активные запросы в ClickHouse**. При выборе нескольких хранилищ в таблице отобразятся активные запросы из каждого выбранного хранилища.

Таблица содержит следующие столбцы:

- **Запущен** – дата и время, когда было запущено выполнение запроса.
- **Создал** – инициатор запроса. Для пользовательских запросов отображается имя пользователя. Для запросов типа **Ресурс** отображается название ресурса.
- **Запрос** – текст SQL-запроса, выполняемого в ClickHouse.

- **Тип** – тип запроса. Доступны следующие типы запросов:
  - **В фоне** – запрос, запущенный пользователем в фоновом режиме по кнопке **Запустить в фоне**.
  - **Ресурс** – служебный SQL-запрос, инициированный ресурсом OSMP в процессе его работы, например, при обработке или анализе данных.
  - **Пользовательский** – SQL-запрос, запущенный пользователем по кнопке **Выполнить запрос** и выполняемый в обычном режиме.
- **Хранилище** – имя хранилища ClickHouse, в контексте которого выполняется запрос.

По кнопке ⚙ вы можете настроить отображаемые столбцы таблицы запросов. При необходимости вы можете принудительно обновить данные по кнопке ↻.

Чтобы отсортировать запросы по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

При необходимости вы можете отменять запросы.

Чтобы отменить выполнение запроса:

1. Откройте таблицу **Активные запросы в ClickHouse**.
2. Установите флажок рядом с нужным запросом и нажмите **Отменить запрос**.

   Откроется окно подтверждения. Вы также можете указать причину отмены выполнения запроса в поле **Укажите причину**.
3. Нажмите **OK**.

Запрос будет отменен и удален из таблицы. При этом автоматически будет создано событие аудита.

Окно Разделы

Создав и установив сервис хранилища, вы можете просмотреть его разделы в таблице **Разделы**.

*Чтобы открыть таблицу **Разделы**:*

1. Войдите в Консоль OSMP и откройте раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем и нажмите **Смотреть разделы**.

Откроется таблица **Разделы**.

Таблица имеет следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные.
- **Создан** – дата создания раздела.
- **Пространство** – название раздела.
- **Размер** – размер раздела.

- **События** – количество хранимых событий.
- **Переход к холодному хранению** – дата, когда данные будут перенесены с кластеров ClickHouse на диски для холодного хранения.
- **Окончание хранения** – дата, когда истекает срок действия раздела. По достижении этого срока раздел и содержащиеся в нем события перестают быть доступны.

Вы можете удалять разделы.

Чтобы удалить раздел:

1. Откройте таблицу **Разделы** (см. выше).
2. Установите флажок рядом с нужным разделом.
3. Выберите пункт **Удалить**.

   Откроется окно подтверждения.
4. Нажмите на кнопку **OK**.

Раздел удален. Разделы для событий аудита удалить невозможно.

Поиск связанных событий

Вы можете искать события, обработанные определенным коррелятором или коллектором.

Чтобы найти события, относящиеся к коррелятору или коллектору:

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным коррелятором или коллектором и нажмите **Перейти к событиям**.

   Откроется новая вкладка браузера с открытым разделом KUMA **События**.
3. Чтобы найти события, нажмите на кнопку **Выполнить запрос**.

   Отобразится таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса>`.

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент OSMP, представляющий собой набор параметров, на основе которых создаются и функционируют сервисы OSMP. Наборы ресурсов для служб собираются из ресурсов.

Ресурсы, объединяемые в набор ресурсов, должны принадлежать к тому же тенанту, что и создаваемый набор ресурсов. Исключением является общий тенант: принадлежащие ему ресурсы можно использовать в наборах ресурсов других тенантов.

Наборы ресурсов для сервисов отображаются в OSMP в разделе **Ресурсы и сервисы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы.
- Корреляторы.
- Хранилища.
- Агенты.

При выборе нужного типа открывается таблица с имеющимися наборами ресурсов для служб этого типа. Таблица содержит следующие столбцы:

- **Название** – имя набора ресурсов. Может использоваться для поиска и сортировки.
- **Последнее обновление** – дата и время последнего обновления набора ресурсов. Может использоваться для сортировки.
- **Создал** – имя пользователя, создавшего набор ресурсов.
- **Описание** – описание набора ресурсов.

Создание хранилища

Хранилище состоит из двух частей: одна часть создается внутри OSMP, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища OSMP представляет собой собранные в кластер узлы ClickHouse. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

Для каждого кластера ClickHouse требуется установить отдельное хранилище.

> Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

> В качестве файловой системы рекомендуется использовать ext4.

Создание хранилища производится в несколько этапов:

1. **Создание набора ресурсов для хранилища в OSMP**
2. **Создание сервиса хранилища в OSMP**
3. **Установка узлов хранилища в сетевой инфраструктуре**

> При создании узлов кластера хранилища убедитесь в сетевой связности системы и откройте используемые компонентами порты.

При изменении параметров хранилища его службу необходимо перезапустить.

Структура кластера ClickHouse

Кластер ClickHouse – логическая группа устройств, обладающих всеми накопленными нормализованными событиями KUMA. Подразумевает наличие одного или нескольких логических *шардов*.

Шард – логическая группа устройств, обладающих некоторой **частью** всех накопленных в кластере нормализованных событий. Подразумевает наличие одной или нескольких *реплик*. Увеличение количества шардов позволяет:

- Накапливать больше событий за счет увеличения общего количества серверов и дискового пространства.
- Поглощать больший **поток** событий за счет распределения нагрузки, связанной со вставкой новых событий.
- Уменьшить время поиска событий за счет распределения поисковых зон между несколькими устройствами.

Реплика – устройство, являющееся членом логического шарда и обладающее одной копией данных этого шарда. Если реплик несколько – копий тоже несколько (данные реплицируются). Увеличение количества реплик позволяет:

- Повысить отказоустойчивость.
- Распределить общую нагрузку, связанную с поиском данных, между несколькими машинами (однако для этой цели лучше увеличить количество шардов).

Кипер – устройство, участвующее в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одно устройство с этой ролью. Рекомендуемое количество устройств с такой ролью – 3. Число устройств, участвующих в координации репликации, должно быть **нечетным**. Роль *кипера* и *реплики* можно совмещать.

Параметры узлов кластера ClickHouse

Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

При создании узлов кластера ClickHouse убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Для каждого узла кластера ClickHouse требуется указать следующие параметры:

- Полное доменное имя (FQDN) – уникальный адрес, по которому должен быть доступен узел. Необходимо указывать FQDN целиком, например `kuma-storage.example.com`.
- Идентификаторы шарда, реплики и кипера – комбинация этих параметров определяет положение узла в структуре кластера ClickHouse и его роль.

Роли узлов

Роли узлов зависят от указанных параметров:

- шард, реплика, кипер – узел участвует в накоплении и поиске нормализованных событий KUMA, а также в координации репликации данных на уровне всего кластера.
- шард, реплика – узел участвует в накоплении и поиске нормализованных событий KUMA.
- кипер – узел **не** накапливает нормализованные события, но участвует в координации репликации данных на уровне всего кластера. Выделенные киперы следует указывать в начале списка в разделе **Ресурсы** → **Хранилища** → <Хранилище> → **Основные параметры** → **Узлы кластера ClickHouse**.

Требования к идентификаторам:

- Если в одном кластере создано несколько шардов, идентификаторы шардов должны быть уникальными в рамках этого кластера.
- Если в одном шарде создано несколько реплик, идентификаторы реплик должны быть уникальными в рамках этого шарда.
- Идентификаторы киперов должны быть уникальными в рамках кластера.

Пример идентификаторов узлов кластера ClickHouse:

- шард 1, реплика 1, кипер 1;
- шард 1, реплика 2;
- шард 2, реплика 1;
- шард 2, реплика 2, кипер 3;
- шард 2, реплика 3;
- кипер 2.

Холодное хранение событий

В OSMP можно настроить перенос устаревших данных с кластера ClickHouse на холодное хранение. Для холодного хранения могут использоваться смонтированные в операционной системе локальные диски, распределенная файловая система Hadoop Distributed File System (HDFS) или облачное хранилище S3 (англ. Simple Storage Service).

Начиная с OSMP версии 2.1, хранящиеся на дисках HDFS данные будут постепенно перенесены в облачное хранилище S3. Поддержка файловой системы HDFS будет прекращена в одном из будущих релизов решения.

Функция холодного хранения включается, если указан хотя бы один диск холодного хранения. Если используется несколько хранилищ, на каждом узле с данными должен быть смонтирован диск холодного хранения или диск HDFS или S3 по пути, указанному в конфигурации хранилища. Если диск холодного хранения не настроен и на сервере в горячем хранилище закончилось место, сервис хранилища остановится. Если есть горячее и холодное хранение и на диске холодного хранения закончилось место, сервис хранилища OSMP остановится. Мы рекомендуем избегать таких ситуаций с помощью добавления пользовательских условий хранения событий в горячем хранилище.

Диски холодного хранения можно добавлять и удалять. Если вы добавили несколько дисков холодного хранения, данные будут записываться на них по стандартному принципу чередования (англ. round-robin) по круговому циклу. Если данные, которые необходимо записать на диск, занимают больше места, чем свободно на этом диске, эти данные и все последующие будут записываться по принципу чередования на следующие диски холодного хранения. Если вы добавили только два диска холодного хранения, данные будут записываться на тот диск, на котором есть свободное место.

После изменения параметров холодного хранения сервис хранилища необходимо перезапустить. Если сервис не запускается, причина будет указана в журнале хранилища.
Перезапуск сервиса также необходим в случае неправильного указания пути к S3-хранилищу. При этом созданный файл *storage.xml* автоматически не удаляется. Вам нужно вручную очистить папку `/opt/kaspersky/kuma/clickhouse/cfg/config.d/` и заново настроить параметры холодного хранилища.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо воссоздать диск с таким же путем (для локальных дисков) или таким же адресом (для дисков HDFS и S3), а затем удалить его из параметров хранилища.

Правила переноса данных на диски холодного хранения

Вы можете настроить условия хранения событий в горячем хранилище кластера ClickHouse, задав ограничение по сроку хранения или по максимальному размеру хранилища. При задействованном холодном хранении OSMP раз в 15 минут и после перезагрузки Ядра проверяет выполнение заданных условий хранения следующим образом:

1. OSMP получает партиции для проверяемого хранилища и группирует их по дискам холодного хранения и пространствам.

2. Для каждого пространства OSMP проверяет, выполняется ли заданное условие хранения.

3. Если условие выполняется (например, в пространстве есть события, хранящиеся дольше указанного срока, или размер хранилища достиг или превышает указанное в условии значение), OSMP переносит все партиции за самую старую дату на диски холодного хранения либо удаляет эти партиции, если диск холодного хранения не настроен или настроен неверно. Это действие повторяется до тех пор, пока в пространстве выполняется заданное условие хранения, например, если после удаления партиций за одну дату размер хранилища все еще превышает заданный в условии максимальный размер.

   При начале и окончании переноса или удалении данных OSMP создает события аудита.

4. Если настроен срок хранения данных в OSMP, при переносе партиций на диски холодного хранения проверяется, выполняются ли на диске заданные условия. Если на диске обнаружены события, хранящиеся дольше срока, заданного в параметре **Время хранения событий**, который рассчитывается с момента их поступления в OSMP, решение удаляет эти события или все партиции за самую старую дату.

   При удалении данных OSMP создает события аудита.

> Если диски кластера ClickHouse заполнены на 97%, самые большие партиции либо автоматически переносятся на диски холодного хранения, либо удаляются, если дисков холодного хранения нет.

Во время переноса данных сервис хранилища продолжает работать, при этом в разделе веб-интерфейса OSMP **Ресурсы** → **Активные сервисы** для него сохраняется зеленый статус. При наведении курсора мыши на значок статуса отображается сообщение о переносе данных. При удалении холодного диска сервис хранилища отображается в желтом статусе.

Особенности хранения событий и доступа к ним

- При использовании для холодного хранения HDFS-дисков необходимо обеспечить защиту данных одним из следующих способов:
  - Настроить отдельный физический интерфейс в сети VLAN, в котором будут расположены только HDFS-диски и кластер ClickHouse.
  - Настроить правила сегментации сети и фильтрации трафика, исключающие прямой доступ к HDFS-диску или перехват трафика к диску со стороны ClickHouse.
- События, находящиеся в кластере ClickHouse и на дисках холодного хранения, одинаково доступны в веб-интерфейсе OSMP. Например, при поиске событий или при просмотре событий, относящихся к алертам.
- Допускается не хранить события или события аудита на дисках холодного хранения. Для этого в параметрах хранилища укажите следующие значения:
  - Если вы не хотите хранить события на дисках холодного хранения, выполните одно из следующих действий:
    - Если в поле **Варианты условий хранения** выбрано условие хранения в гигабайтах или процентах, в поле **Время хранения событий** укажите значение `0`.
    - Если в поле **Варианты условий хранения** выбрано условие хранения в днях, в поле **Время хранения событий** укажите такое же значение дней, как в поле **Варианты условий хранения**.
  - Если вы не хотите хранить события аудита на дисках холодного хранения, в поле **Срок холодного хранения событий аудита** укажите значение `0` (дней).

Особенности использования HDFS-дисков

- Перед подключением HDFS-дисков на них необходимо создать директории для каждого узла кластера ClickHouse в формате `<устройство HDFS-диска>/<идентификатор шарда>/<идентификатор реплики>`. Например, если кластер состоит из двух узлов, на которых расположены две реплики одного шарда, необходимо создать следующие директории:

  - hdfs://hdfs-example-1:9000/clickhouse/1/1/

  - hdfs://hdfs-example-1:9000/clickhouse/1/2/

  События из узлов кластера ClickHouse будут переноситься в директории, в названии которых указаны идентификаторы их шарда и реплики. Если изменить эти параметры узла и при этом не создать соответствующую директорию на HDFS-диске, события при переносе могут быть потеряны.

- HDFS-диски, добавленные к хранилищу, работают в режиме JBOD. Это означает, что при отказе одного из дисков будет потерян доступ к хранилищу. При использовании HDFS следует учитывать необходимость отказоустойчивости и настроить RAID, а также хранение данных из разных реплик на различных устройствах.

- Скорость записи событий в HDFS, как правило, ниже скорости записи событий на локальные диски. Скорость доступа к событиям в HDFS, как правило, значительно ниже скорости доступа к событиям на локальных дисках. При использовании одновременно локальных дисков и HDFS-дисков запись будет происходить в них по очереди.

- HDFS используется только в качестве распределенного хранилища файловых данных ClickHouse. Для сжатия данных используются механизмы сжатия ClickHouse, а не HDFS.

- Сервер ClickHouse должен иметь доступ к соответствующему хранилищу HDFS с правами на запись.

Удаление дисков холодного хранения

Перед физическим отключением дисков холодного хранения необходимо удалить эти диски из параметров хранилища.

Чтобы удалить диск из параметров хранилища:

- В OSMP перейдите в раздел **Ресурсы и сервисы** → **Хранилища** и выберите нужное хранилище.

  Откроется хранилище.

- В окне в разделе **Диски холодного хранения** в блоке параметров нужного диска нажмите **Удалить диск**.

  Данные с удаляемого диска автоматически начинают переноситься на другие диски холодного хранения или, если их нет, в кластер ClickHouse. В процессе переноса данных значок статуса хранилища светится желтым цветом. При начале и окончании переноса данных создаются события аудита.

- После завершения переноса событий диск автоматически удаляется из параметров хранилища. Теперь его можно безопасно отключить.

На удаляемых дисках могут оставаться события. Если вы хотите их удалить, вы можете, например, вручную удалить партиции с данными с помощью команды DROP PARTITION.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо создать диск с таким же путем (для локальных дисков) или таким же адресом (для HDFS-дисков), а затем удалить его из параметров хранилища.

Отключение, архивирование и подключение партиций

Если вы хотите оптимизировать дисковое пространство и ускорить выполнение запросов в OSMP, вы можете отключить в ClickHouse партиции с данными, архивировать партиции или перенести их на носитель. При необходимости вы можете снова подключить необходимые партиции и выполнить обработку данных.

Отключение партиций

Чтобы отключить партиции, выполните следующие шаги:

1. Определите шард, на всех репликах которого вы планируете отключить партицию.

2. Получите идентификатор партиции с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   В приведенном примере в результате выполнения команды будет получен идентификатор партиции от 30 ноября 2023 года.

3. На каждой реплике шарда отключите партицию с помощью следующей команды, указав требуемый идентификатор:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<идентификатор партиции>'"
   ```

В результате партиция отключена на всех репликах шарда. Теперь вы можете перенести директорию с данными на носитель или заархивировать партицию.

Архивирование партиций

Чтобы архивировать отключенные партиции:

1. Найдите отключенную партицию в дисковой подсистеме сервера:

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <идентификатор отключенной партиции>\*
   ```

2. Перейдите в директорию detached с отключенной партицией и, находясь в директории detached, выполните архивирование:

   ```
   sudo cd <путь к директории detached, содержащую отключенную партицию>
   sudo zip -9 -r detached.zip *
   ```

   Например:

   ```
   sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   sudo zip -9 -r detached.zip *
   ```

Архивирование партиции выполнено.

Подключение партиций

Чтобы подключить архивные партиции к OSMP:

1. Увеличьте значение параметра **Срок хранения**.

   OSMP удаляет данные на основании даты, указанной в поле Timestamp, когда событие получено, и на основании значения параметра **Срок хранения**, которое вы задали для хранилища.

   Перед тем как выполнять восстановление архивных данных, убедитесь, что значение параметра **Срок хранения** перекрывает дату из поля Timestamp. В противном случае, архивные данные будут удалены в течение 1 часа.

2. Поместите архивную партицию в раздел detached вашего хранилища и распакуйте архив:

   ```
   sudo unzip detached.zip -d <путь к директории detached>
   ```

   Например:

   ```
   sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

3. Выполните команду подключения партиции:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<идентификатор партиции>'"
   Повторите шаги распаковки архива и подключения партиции на каждой реплике шарда.
   ```

В результате архивная партиция подключена и события снова доступны для поиска.

Создание набора ресурсов для хранилища

Сервис хранилища в веб-интерфейсе OSMP создается на основе набора ресурсов для хранилища.

Чтобы создать набор ресурсов для хранилища в веб-интерфейсе OSMP:

1. В OSMP в разделе **Ресурсы** → **Хранилища** нажмите **Создать**.

   Откроется окно **Создание хранилища**.

2. На вкладке **Основные параметры** в поле **Название хранилища** введите уникальное имя создаваемого сервиса. Имя должно содержать от 1 до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.

4. В раскрывающемся списке **Теги** выберите теги для создаваемого набора ресурсов.

   В списке отображаются все доступные теги, созданные в тенанте ресурса и Общем тенанте. Вы может найти тег в списке, начав вводить его название в поле. Если тега, который вы ввели, не существует, вы можете нажать **`Enter`** или **Добавить**, чтобы создать его.

5. В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

6. В поле **Варианты условий хранения** выберите для хранилища условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно. Условие будет применено к пространству по умолчанию и к событиям из удаленных пространств.

   По умолчанию ClickHouse перемещает события на диски холодного хранения или удаляет их, если заполнено более 97% хранилища. В OSMP при создании хранилища также используется дополнительное условие хранения **365 дней**. Вы можете настроить пользовательские условия хранения для более устойчивой работы хранилища.

   Чтобы задать условие хранения, выполните одно из следующих действий:

   - Если вы хотите ограничить срок хранения событий, в раскрывающемся списке выберите **Дни** и в поле укажите максимальный срок хранения событий в днях в кластере горячего хранилища ClickHouse.

     По истечении указанного срока события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение – 1. Значение по умолчанию – 365.

     Для хранилища [OOTB] Storage по умолчанию установлен срок хранения событий два дня. Если вы хотите использовать это хранилище, при необходимости вы можете изменить для него условие хранения событий.

   - Если вы хотите ограничить максимальный размер хранилища, в раскрывающемся списке выберите **ГБ** и в поле укажите максимальный размер хранилища в гигабайтах.

     Когда размер хранилища достигнет указанного значения, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение и значение по умолчанию – 1 ГБ.

   - Если вы хотите ограничить размер хранилища относительно объема диска, который доступен хранилищу, в раскрывающемся списке выберите **Проценты** и укажите максимальный размер хранилища в процентах от доступного объема диска.

     > Информацию о доступном объеме диска вы можете получить из ClickHouse, отправив запрос `'SELECT hostname(), name, total_space FROM system.disks'`.

     Когда размер хранилища достигнет указанной доли от доступного ему размера диска, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Допустимые значения – от 1 до 95. Значение по умолчанию – 80. Если вы хотите использовать проценты для всех пространств хранилища, сумма процентов в условиях всех пространств не может превышать 95, но рекомендуется указывать ограничение не более 90% включительно для всего хранилища или для отдельных пространств.

     Не рекомендуется указывать значение меньше 5%, так как в этом случае возрастает вероятность потери данных в хранилище.

Если хранилище организовано в виде кластера из нескольких серверов, объем занятого дискового пространства определяется отдельно для каждого сервера. Данные для хранения могут распределяться между дисками на серверах неравномерно. В OSMP события будут перемещаться на диски холодного хранения или удаляться при достижении максимального размера хранилища *на одном из серверов в кластере*.

Механизм определения размера занятого пространства в хранилище

Определение размера занятого пространства в хранилище осуществляется следующим образом:

1. Информация о состоянии дисков и партиций KUMA получается со всех доступных реплик.

2. Если занятое пространство превышает установленные значения, KUMA осуществляет действия в зависимости от типа хранения данных: горячее или холодное.

   При горячем хранении данных для каждого доступного узла и пространства осуществляются следующие действия:

   a. Рассчитывается суммарный размер партиций этого пространства на реплике.

   b. Рассчитывается максимальный размер пространства на реплике:

      - Если установлено абсолютное значение для размера хранилища в ГБ, максимальный размер пространства на реплике рассчитывается следующим образом:

        `<максимальный размер пространства> = <установленное пороговое значение> / <число реплик в кластере>`

        Например, для кластера из трех шардов, в каждом из которых находятся две реплики, и установлено пороговое значение 6 ГБ, максимальный объем данных на реплике – 1 ГБ.

      - Если установлено относительное значение для размера хранилища в процентах, максимальный размер пространства на реплике рассчитывается следующим образом:

        `<максимальный размер пространства> = <размер пространства на реплике> / <размер диска реплики> * 100%`

        Размер диска реплики не включает в себя пространство, зарезервированное для `ext4`.

   Если установленное пороговое значение превышено, партиции на хосте удаляются или переносятся в холодное хранилище. Партиции удаляются на всех шардах.

   При холодном хранении данных для каждого доступного пространства партиции удаляются в соответствии с установленным значением времени хранения событий в KUMA (TTL).

7. Если вы хотите использовать дополнительное условие хранения, нажмите на кнопку **Добавить условие хранения** и укажите дополнительное условие хранения, как описано в пункте 6.

   Вы можете добавить не более двух условий и сочетать только условия следующих типов:

   - дни и размер хранилища в ГБ;

   - дни и размер хранилища в процентах.

   Если вы хотите удалить условие хранения, нажмите на значок крестика возле этого условия.

8. В поле **Срок хранения событий аудита** укажите, в течение какого количества дней вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: `365`.

9. При необходимости холодного хранения данных введите сроки хранения событий:

   - **Время хранения событий** – общая длительность хранения событий в OSMP с момента поступления, в днях. По истечении указанного срока события будут автоматически удалены с диска холодного хранения. Значение по умолчанию – 0.

     Время хранения событий рассчитывается как сумма времени хранения событий в кластере горячего хранилища ClickHouse до наступления условия, заданного в параметре **Варианты условий хранения**, и времени хранения событий на диске холодного хранения. После наступления одного из условий хранения партиция данных за самую старую дату перемещается на диск холодного хранения и находится там до истечения времени хранения событий в OSMP.

     В зависимости от заданного условия хранения время хранения будет следующим:

     - Если вы задали условие хранения в днях, значение параметра **Время хранения событий** должно быть строго больше количества дней, указанного в условии хранения. Вы можете рассчитать срок холодного хранения событий как **Время хранения событий** минус количество дней, указанное в параметре **Варианты условий хранения**.

       Если вы не хотите хранить события на диске холодного хранения, в параметре **Время хранения событий** вы можете указать такое же количество дней, как в условии хранения.

     - Если вы задали условие хранения в размере диска (точном или в процентах), минимальное значение параметра **Время хранения событий** – 1. Срок холодного хранения событий будет рассчитан как **Время хранения событий** минус количество дней с поступления события до момента выполнения условия и заполнения раздела диска, но до выполнения условия невозможно рассчитать точный срок. В этом случае рекомендуется указывать относительно большое значение параметра **Время хранения событий**, чтобы избежать удаления событий.

       Если вы не хотите хранить события на диске холодного хранения, в параметре **Время хранения событий** вы можете указать значение 0.

   - **Срок холодного хранения событий аудита** – количество дней хранения событий аудита. Минимальное значение – 0.

   Параметры **Время хранения событий** и **Срок холодного хранения событий аудита** становятся доступны, только после того как вы добавили хотя бы один диск холодного хранения.

10. При необходимости изменения параметров ClickHouse в поле **Переопределение параметров ClickHouse** вставьте строки с параметрами из XML-файла конфигурации ClickHouse /opt/kaspersky/kuma/clickhouse/cfg/config.xml. Указание корневых элементов <yandex>, </yandex> не требуется. Переданные в поле параметры конфигурации будут использоваться вместо параметров по умолчанию.

    Пример:

    <merge_tree>

    <parts_to_delay_insert>600</parts_to_delay_insert>

    <parts_to_throw_insert>1100</parts_to_throw_insert>

    </merge_tree>

    Если вы хотите ускорить работу графа и поиск угроз, вы можете изменить алгоритм сжатия ClickHouse. По умолчанию используется алгоритм ZSTD. Значение по умолчанию можно заменить на LZ4. Для этого в поле **Переопределение параметров ClickHouse** укажите значение алгоритма сжатия следующим образом:

```
<compression>
  <case>
```

```
    <method>lz4</method>
  </case>
<compression>
```

> Алгоритм LZ4 будет применяться решением после перезагрузки сервиса хранилища. Все события, которые сохранялись в хранилище до изменения алгоритма, останутся сжатыми с помощью алгоритма ZSTD.

11. С помощью переключателя **Отладка** укажите, будет ли включено логирование ресурса. Если вы хотите для всех компонентов KUMA регистрировать в журнале только ошибки, выключите отладку. Если вы хотите получать детализированные данные в журналах, включите отладку.

12. При необходимости в разделе **Узлы кластера ClickHouse** добавьте в хранилище узлы кластера ClickHouse.

    Узлов может быть несколько. Узлы можно добавить с помощью кнопки **Добавить узел** и удалить, нажав на значок крестика в блоке нужного узла.

    Доступные параметры:

    - В поле **FQDN** укажите полное доменное имя добавляемого узла. Например, `kuma-storage-cluster1-server1.example.com`.

    - В полях **Идентификатор шарда**, **Идентификатор реплики** и **Идентификатор кипера** укажите роль узла в кластере ClickHouse. Идентификаторы шарда и кипера должны быть уникальными в рамках кластера, идентификатор реплики должен быть уникальным в рамках шарда. Ниже показан пример заполнения раздела **Узлы кластера ClickHouse** для хранилища с выделенными киперами в распределенной схеме установки. Вы можете адаптировать пример для своих потребностей.

Распределенная схема установки

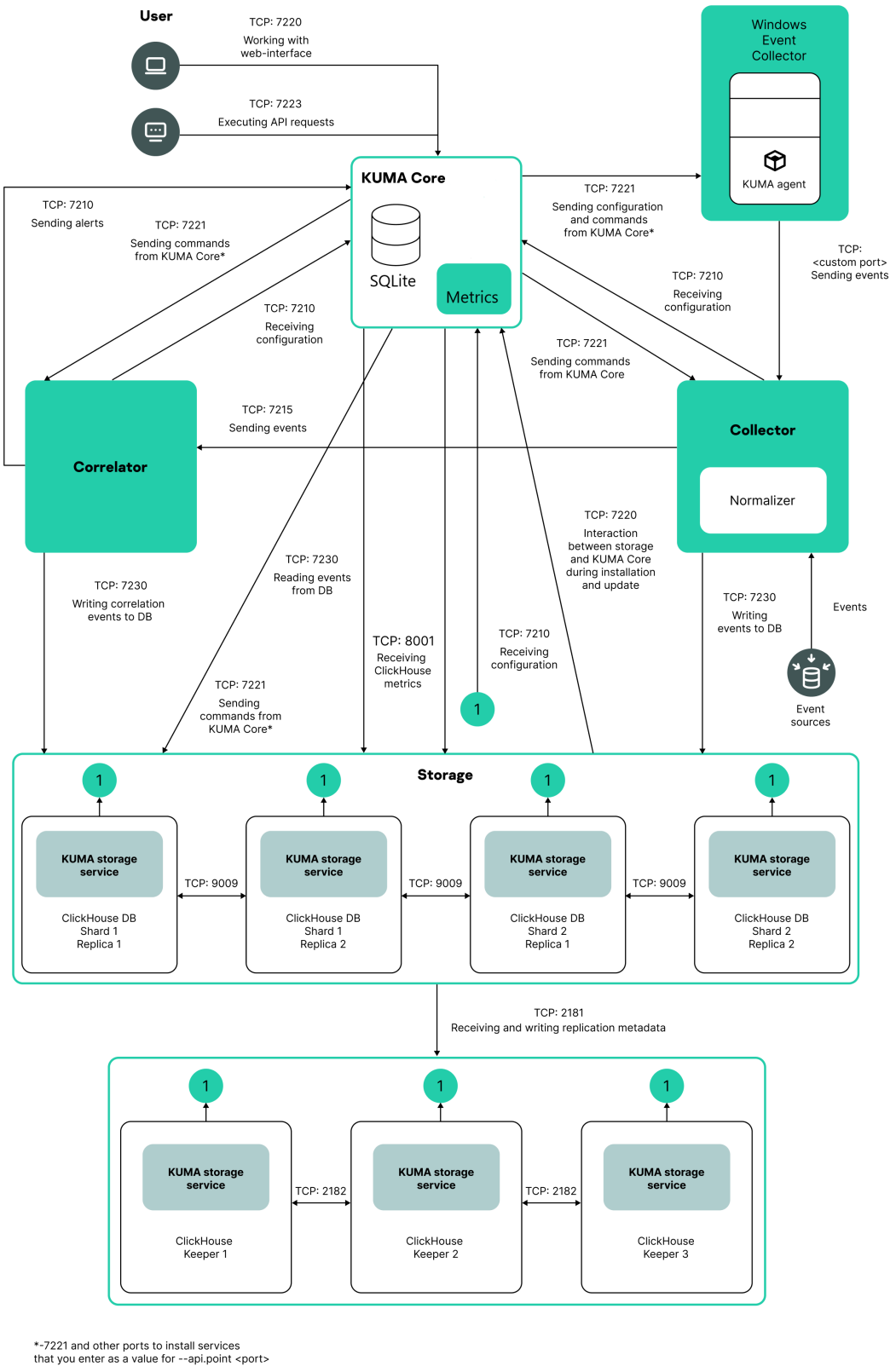


Схема распределенной установки

Пример:

Узлы кластера ClickHouse

Полное доменное имя: kuma-storage-cluster1-server1.example.com

Идентификатор шарда: 0

Идентификатор реплики: 0
Идентификатор кипера: 1
Полное доменное имя: kuma-storage-cluster1server2.example.com
Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 2
Полное доменное имя: kuma-storage-cluster1server3.example.com
Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 3
Полное доменное имя: kuma-storage-cluster1server4.example.com
Идентификатор шарда: 1
Идентификатор реплики: 1
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server5.example.com
Идентификатор шарда: 1
Идентификатор реплики: 2
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server6.example.com
Идентификатор шарда: 2
Идентификатор реплики: 1
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server7.example.com
Идентификатор шарда: 2
Идентификатор реплики: 2
Идентификатор кипера: 0

13. При необходимости в разделе **Пространства** добавьте в хранилище пространства, по которым вы хотите распределять хранимые события.

    Пространств может быть несколько. Пространства можно добавить с помощью кнопки **Добавить пространство** и удалить, нажав на значок крестика в блоке нужного пространства.

    Доступные параметры:

    - В поле **Название** укажите название пространства: от 1 до 128 символов в кодировке Unicode.

    - В поле **Варианты условий хранения** выберите для пространства условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно. В OSMP при добавлении пространства используется условие хранения **365 дней**.

      Чтобы задать условие хранения для пространства, выполните одно из следующих действий:

      - Если вы хотите ограничить срок хранения событий, в раскрывающемся списке выберите **Дни** и в поле укажите максимальный срок хранения событий в днях в кластере горячего хранилища ClickHouse.

        По истечении указанного срока события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение – 1. Значение по умолчанию – 365.

      - Если вы хотите ограничить максимальный размер пространства хранилища, в раскрывающемся списке выберите **ГБ** и в поле укажите максимальный размер пространства в гигабайтах.

        Когда размер пространства достигнет указанного значения, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение и значение по умолчанию – 1.

- Если вы хотите ограничить размер пространства хранилища относительно объема диска, который доступен хранилищу, в раскрывающемся списке выберите **Проценты** и в поле укажите максимальный размер пространства в процентах от объема диска, доступного хранилищу. В этом случае условие также может сработать при уменьшении доступного хранилищу объема диска.

  Когда размер пространства достигнет указанной доли от объема диска, доступного хранилищу, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Допустимые значения – от 1 до 95. Значение по умолчанию – 80. Если вы хотите использовать проценты для всех пространств хранилища, сумма процентов в условиях всех пространств не может превышать 95, но рекомендуется указывать ограничение не более 90% включительно для всего хранилища или для отдельных пространств.

  Мы не рекомендуем указывать малые значения процентов, так как в этом случае возрастает вероятность потери данных в хранилище.

При использовании размера в качестве условия хранения требуется следить, чтобы суммарный размер пространств, указанный в условиях хранения не превышал физический размер хранилища, иначе при запуске сервиса отобразится ошибка.

В условиях хранения с ограничением размера для всех пространствах хранилища используйте одинаковые единицы изменения (только в гигабайтах или только в процентах). Иначе, если для одного пространства условие задано в процентах, а для другого в гигабайтах, хранилище может переполниться из-за несоответствия значений и данные будут потеряны.

- При необходимости сделать пространство неактивным в случае, если оно устарело и больше не является актуальным, установите флажок **Только для чтения**.

  В этом случае новые события больше не будут попадать в пространство. Чтобы снова сделать пространство активным, снимите флажок **Только для чтения**. По умолчанию флажок снят.

- При необходимости в поле **Время хранения событий** укажите общую длительность хранения событий в KUMA с момента поступления, в днях. По истечении указанного срока события будут автоматически удалены с диска холодного хранения. Значение по умолчанию – 0.

  Время хранения событий рассчитывается как сумма времени хранения событий в кластере горячего хранилища ClickHouse до наступления условия, заданного в параметре **Варианты условий хранения**, и времени хранения событий на диске холодного хранения. После наступления одного из условий хранения партиция данных за самую старую дату перемещается на диск холодного хранения и находится там до истечения времени хранения событий в OSMP.

  В зависимости от заданного условия хранения время хранения будет следующим:

  - Если вы задали условие хранения в днях, значение параметра **Время хранения событий** должно быть строго больше количества дней, указанного в условии хранения. Срок холодного хранения событий будет рассчитан как **Время хранения событий** минус количество дней, указанное в параметре **Варианты условий хранения**.

    Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать такое же количество дней, как в условии хранения.

- Если вы задали условие хранения в размере диска (точном или в процентах), минимальное значение параметра **Время хранения событий** – 1. Срок холодного хранения событий будет рассчитан как **Время хранения событий** минус количество дней с поступления события до момента выполнения условия и заполнения раздела диска, но до выполнения условия невозможно рассчитать точный срок. В этом случае рекомендуется указывать относительно большое значение параметра **Время хранения событий**, чтобы избежать удаления событий.

  Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать значение 0.

Параметр **Время хранения событий** становится доступен, только после того как вы добавили хотя бы один диск холодного хранения.

- В разделе **Параметры фильтра** можно задать условия определения событий, которые будут помещаться в это пространство. Чтобы создать фильтр, в раскрывающемся списке **Фильтр** выберите существующий фильтр или **Создать**.

  Создание фильтра в ресурсах

  Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

  Чтобы создать фильтр:

  1. В раскрывающемся списке **Фильтр** выберите **Создать**.

  2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

  3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

  4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

     a. Нажмите на кнопку **Добавить условие**.

     b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **Оператор** выберите оператор.

     Операторы фильтров

     - **=** – левый операнд равен правому операнду.

     - **<** – левый операнд меньше правого операнда.

     - **<=** – левый операнд меньше или равен правому операнду.

     - **>** – левый операнд больше правого операнда.

- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

После создания сервиса пространства можно просматривать и удалять в параметрах набора ресурсов хранилища.

> Нет необходимости создавать отдельное пространство для событий аудита. События этого типа (Type=4) автоматически помещаются в отдельное пространство Audit со сроком хранения не менее 365 дней, которое недоступно для редактирования или удаления из веб-интерфейса OSMP.

14. При необходимости в разделе **Диски холодного хранения** добавьте в хранилище диски, на которые вы хотите переносить события на длительное хранение из кластера ClickHouse.

    Дисков может быть несколько. Диски можно добавить с помощью кнопки **Добавить диск** и удалить с помощью кнопки **Удалить диск**.

    Доступные параметры:

- В раскрывающемся списке **Тип** выберите тип доменного имени подключаемого диска:
  - **Локальный** – для дисков, смонтированных в операционной системе как директории.
  - **HDFS** – для дисков распределенной файловой системы Hadoop Distributed File System.
  - **S3** – для дисков облачного хранилища S3, использующихся в KUMA.

  > Начиная с версии 4.2, данные, хранящиеся на дисках HDFS, будут постепенно перенесены на диски хранилища S3. Поддержка файловой системы HDFS будет прекращена в одном из будущих релизов решения.

- В поле **Название** укажите название диска. Название должно содержать от 1 до 128 символов в кодировке Unicode.

  > Вы не можете изменить название S3-диска без изменения пути к этому диску.

- Если в качестве типа доменного имени диска вы выбрали **Локальный**, в поле **Путь** введите одно из значений:

  - Если сервис хранилища развернут локально, введите абсолютный путь директории смонтированного локального диска. Путь должен начинаться и оканчиваться символом "/".

    > Владельцем директории смонтированного локального диска должен быть пользователь KUMA.

  - Если сервис хранилища развернут в кластере Kubernetes, введите путь: `/opt/cold/`. В директорию `/opt/cold/` будет монтирована директория `/opt/lvp/cold/` того узла кластера Kubernetes, на котором будет развернут сервис хранилища.

- Если в качестве типа доменного имени диска вы выбрали **HDFS**, в поле **Хост** введите путь к HDFS (например, `hdfs://hdfs1:9000/clickhouse/`).

- Если в качестве типа доменного имени диска вы выбрали **S3**, укажите значения следующих параметров:

  - В поле **Хост** укажите адрес S3-хранилища (например, `https://www.company.com/clickhouse/storagefolder/`).

    Правила указания адреса хранилища S3

    При указании адреса S3-хранилища нужно выполнять следующие требования:

    - Адрес указывается в формате URL, например:
      `https://<веб-адрес/IP-адрес сервера>/<путь к диску>/`
    - Адрес должен оканчиваться символом "/".
    - Максимальная длина – 2048 символов.
    - Использование кириллических символов не допускается.

    > Вы не можете изменить адрес диска хранилища S3 без изменения названия диска.

  - В поле **Секрет** укажите секрет для доступа к хранилищу S3. Вы можете выбрать секрет в раскрывающемся списке или создать новый секрет, нажав **Создать**.

15. В блоке **Настройка резервного копирования и восстановления** настройте следующие параметры:

    a. В поле **Резервное копирование хранилища** укажите путь хранения файла резервной копии. Например, /mnt/data.

    Требования к пути:

    - Путь должен существовать и быть одинаковым на всех узлах кластера хранения.
    - У пользователя должны быть права на чтение, запись и запуск файлов в указанной директории.
    - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например, /backup.
    - Название директории не должно содержать точку.

- **Путь не должен содержать следующие префиксы**.

  Префиксы, которые невозможно использовать при указании путей к файлам:

  - `/*`
  - `/bin`
  - `/boot`
  - `/dev`
  - `/etc`
  - `/home`
  - `/lib`
  - `/lib64`
  - `/proc`
  - `/root`
  - `/run`
  - `/sys`
  - `/tmp`
  - `/usr/*`
  - `/usr/bin/`
  - `/usr/local/*`
  - `/usr/local/sbin/`
  - `/usr/local/bin/`
  - `/usr/sbin/`
  - `/usr/lib/`
  - `/usr/lib64/`
  - `/var/*`
  - `/var/lib/`
  - `/var/run/`
  - `/opt/kaspersky/kuma/`

Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.

Файлы по указанным ниже путям доступны:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

По указанному пути будут автоматически созданы две директории: **backup** и **restore**.

Если путь не указан, резервное копирование по расписанию, ручное резервное копирование, восстановление из резервной копии и импорт будут недоступны.

b. Если вы хотите настроить резервное копирование по расписанию, включите переключатель **Резервное копирование по расписанию**.

c. В поле **Резервное копирование через несколько дней** укажите целое число, которое означает, через сколько дней после создания партиции следует выполнять резервное копирование. Например, при значении **1** резервное копирование будет выполняться для партиции, созданной позавчера.

d. В раскрывающемся списке **Реплики** выберите одну реплику, для которой следует выполнить резервное копирование. При выборе нескольких реплик одного шарда произойдет дублирование данных.

e. В блоке **Партиции** нажмите **Добавить партицию** и настройте следующие параметры:

   a. В раскрывающемся списке **Тенант** выберите тенант, в котором находится партиция для резервного копирования.

   b. В раскрывающемся списке **Пространства** выберите одно или несколько пространств хранилища, которые принадлежат партиции для резервного копирования. Если значение не указано, будет выполнено резервное копирование партиции целиком.

   Вы можете настроить параметры для нескольких партиций. При необходимости нажмите **Добавить партицию** и настройте параметры в появившихся полях для новой партиции. Например, если вы хотите выполнить резервное копирование пространства **Audit** и у вас 10 тенантов, необходимо настроить резервное копирование отдельно для каждого тенанта.

16. Перейдите на вкладку **Дополнительные параметры** и заполните следующие поля:

- В поле **Размер буфера** укажите размер буфера в байтах, при достижении которого следует передать события в базу. Значение по умолчанию – 128 МБ. Максимального значения нет. Если на виртуальной машине меньше свободной памяти, чем заданное значение **Размер буфера**, OSMP установит ограничение в 128 МБ.

  Если ожидаемый трафик на сервис хранилища будет больше 1 Гбит/сек, рекомендуется изменить значение параметра **Размер буфера** в байтах в соответствии с известным вам значением и указать значение параметра **Интервал очистки буфера** равное 2.

  Значение параметра **Размер буфера** можно определить опытным путем. Если на метрике хранилища **Insert QPS** показатель превышает 1 и видно, что увеличивается очередь запросов, воспользуйтесь рекомендациями по расчету и корректировке значения параметра **Размер буфера**, приведенными в статье Просмотр метрик OSMP в разделе Insert QPS.

- В поле **Максимальный размер буфера** укажите максимальный размер буфера в байтах. Значение по умолчанию – 256 МБ.

По умолчанию события записываются в базу данных раз в секунду. Если поток событий возрастает и события начинают записываться чаще, чем раз в секунду, размер буфера автоматически увеличивается. Буфер увеличится максимум в три раза от значения в поле **Размер буфера**, но не может превысить значения в поле **Максимальный размер буфера**. После увеличения размера буфера при нормализации нагрузки размер не меняется, автоматическое уменьшение буфера не предусмотрено.

Если вы укажете значение в поле **Максимальный размер буфера** меньшим или равным значению в поле **Размер буфера**, то размер буфера не изменится.

При перезапуске сервиса хранилища увеличенный размер буфера сбрасывается до значения в поле **Размер буфера**.

- В поле **Интервал очистки буфера** укажите интервал в секундах, в течение которого OSMP будет ждать заполнения буфера. Если буфер не заполнен, но указанное время прошло, OSMP передает события в базу. Значение по умолчанию 1 с.

- В поле **Требуемый объем памяти** укажите минимальный размер свободной оперативной памяти в байтах. Значение по умолчанию — 128 МБ.

  Если на узле, на котором установлено хранилище, свободной оперативной памяти окажется меньше указанного значения, запрос на запись событий в базу данных вернет ошибку, события будут записаны позже. Ограничение размера памяти позволяет избежать ситуации, когда память переполняется, если по какой-либо причине запись событий в базу данных блокируется и данные начинают накапливаться в памяти.

- В поле **Ограничение размера дискового буфера** укажите значение в байтах. Дисковый буфер используется для временного размещения тех событий, которые не удалось отправить для дальнейшей обработки или хранения. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер. Значение по умолчанию: 10 ГБ.

- С помощью переключателя **Дисковый буфер** включите или выключите использование дискового буфера. По умолчанию дисковый буфер включен.

- С помощью переключателя **Запись в локальную таблицу базы данных** включите или выключите запись в локальную таблицу базы данных. По умолчанию запись выключена.

  Если вы включите запись, она будет выполняться только на том узле, на котором установлено хранилище. Рекомендуется использовать эту функцию только при условии, что у вас настроена балансировка на коллекторе и/или коррелятоpe: в коллекторе и/или коррелятоpe на шаге **6. Маршрутизация** в разделе **Дополнительные настройки** в поле **Политика выбора URL** установлено значение **По очереди**.

  Если вы выключите запись, данные распределяются по шардам кластера.

- При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.

- Переключатель **Периодическое создание дампа** используется по запросу Службы технической поддержки для генерации отчетов по потреблению ресурсов (например CPU, RAM) в виде дампов.

- В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля вы можете уточнить у Службы технической поддержки.

Набор ресурсов для хранилища создан и отображается в разделе **Ресурсы** → **Хранилища**. Теперь можно создать сервис хранилища.

Создание службы хранилища в OSMP

Когда набор ресурсов для хранилища создан, можно перейти к созданию службы хранилища в KUMA.

Чтобы создать службу хранилища в OSMP:

1. В Консоли KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для хранилища и нажмите **Создать сервис**.

Сервис хранилища создан в OSMP и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь службы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор службы.

Установка хранилища в сетевой инфраструктуре OSMP

Чтобы создать хранилище:

1. Войдите на сервер, на котором вы хотите установить службу.

2. Создайте папку /opt/kaspersky/kuma/.

3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the
KUMA Core CA certificate> --id <service ID> --install
```

   где:

   - <FQDN> – полное доменное имя сервера Ядра KUMA.

   - <port> – порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)

   - <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

     Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

     Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.

Пример:

```
sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --install
```

> При развертывании нескольких сервисов KUMA на одном устройстве в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port < порт >`. По умолчанию используется значение `--api.port 7221`.

5. Повторите шаги 1–2 для каждого узла хранилища.

Хранилище установлено.

Резервное копирование, восстановление и импорт партиций

В OSMP пользователям с ролью Главный администратор доступны следующие действия:

- Резервное копирование партиций по расписанию.
- Резервное копирование партиций вручную.
- Восстановление партиций из резервной копии.
- Импорт партиций из стороннего экземпляра OSMP.

Вы можете настроить и использовать холодное хранение событий и резервное копирование партиций одновременно.

Вы можете просмотреть статус выполнения резервного копирования, восстановления и импорта партиций в событии аудита. Также после запуска резервного копирования партиций вручную, восстановления партиций из резервной копии и импорта партиций из стороннего экземпляра OSMP в разделе **Диспетчер задач** создается соответствующая задача.

Резервное копирование партиций по расписанию

Возможность настроить резервное копирование партиций по расписанию доступна пользователям с ролью Главный администратор.

Чтобы настроить резервное копирование по расписанию:

1. В главном меню перейдите в раздел Мониторинг → Ресурсы и сервисы → **Активные сервисы** и откройте действующее хранилище для настройки параметров.

2. В открывшемся окне **Редактирование хранилища** на вкладке **Основные параметры** в блоке **Настройка резервного копирования и восстановления** настройте следующие параметры:

   a. В поле **Резервное копирование хранилища** укажите путь хранения файла резервной копии. Например, /mnt/data. Если путь хранения не указан, выполнить резервное копирование невозможно.

   b. Включите переключатель **Резервное копирование по расписанию**.

   c. В поле **Резервное копирование через несколько дней** укажите целое число, которое означает, через сколько дней после создания партиции следует выполнять резервное копирование. Например, при значении **1** резервное копирование будет выполняться для партиции, созданной позавчера.

   d. В раскрывающемся списке **Реплики** выберите одну реплику, для которой следует выполнить резервное копирование. При выборе нескольких реплик одного шарда произойдет дублирование данных.

      Если в кластере используется несколько шардов, список **Реплики** будет содержать только те реплики, идентификаторы которых указаны во всех шардах.

3. В блоке **Партиции** нажмите **Добавить партицию** и настройте следующие параметры:

   a. В раскрывающемся списке **Тенант** выберите тенант, в котором находится партиция для резервного копирования.

   b. В раскрывающемся списке **Пространства** выберите одно или несколько пространств хранилища, которые принадлежат партиции для резервного копирования. Если значение не указано, будет выполнено резервное копирование партиции целиком.

      Вы можете настроить параметры для нескольких партиций. При необходимости нажмите **Добавить партицию** и настройте параметры в появившихся полях для новой партиции. Например, если вы хотите выполнить резервное копирование пространства **Audit** и у вас 10 тенантов, необходимо настроить резервное копирование отдельно для каждого тенанта.

4. Нажмите **Сохранить**.

После сохранения параметров по указанному пути будет автоматически созданы директории **backup** и **restore**. В директории **backup** будут автоматически созданы вложенные директории с идентификатором тенанта и идентификатором пространства. Например, если вы указали путь хранения резервной копии /mnt/data, полный путь к файлу резервной копии будет выглядеть следующим образом: /mnt/data/backup/<идентификатор тенанта>/<идентификатор пространства хранилища>/<дата создания партиции>.zip. Если вам необходимо узнать идентификатор тенанта или пространства, вы можете перейти в раздел **События**, открыть карточку события и просмотреть информацию.

Для восстановления из резервной копии необходимо будет перенести файл резервной копии в директорию **restore**.

Резервное копирование партиций по расписанию настроено. В случае неуспешного выполнения резервного копирования будет создано соответствующее событие аудита, сервису хранилища в разделе **Активные сервисы** будет присвоен желтый статус и при наведении курсора мыши на желтый статус будет отображаться сообщение об ошибке. При очередном запуске резервного копирования по расписанию сначала происходит попытка резервного копирования старых данных.

Резервное копирование партиций вручную

Выполнение резервного копирования партиций вручную доступно пользователям с ролью Главный администратор.

Чтобы создать резервную копию партиции вручную:

1. В главном меню перейдите в раздел Мониторинг → Ресурсы и сервисы → **Активные сервисы** и откройте действующее хранилище для настройки параметров.

2. В открывшемся окне **Редактирование хранилища** на вкладке **Основные параметры** в блоке **Настройка резервного копирования** в поле **Резервное копирование хранилища** укажите путь хранения файла резервной копии. Например, /mnt/data. Убедитесь, что у пользователя kuma есть права доступа к указанной директории.

   Требования к пути:

   - Путь должен существовать и быть одинаковым на всех узлах кластера хранения.
   - У пользователя должны быть права на чтение, запись и запуск файлов в указанной директории.
   - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например, /backup.
   - Название директории не должно содержать точку.
   - **Путь не должен содержать следующие префиксы**.

     Префиксы, которые невозможно использовать при указании путей к файлам:

     - `/*`
     - `/bin`
     - `/boot`
     - `/dev`
     - `/etc`
     - `/home`
     - `/lib`
     - `/lib64`
     - `/proc`
     - `/root`
     - `/run`
     - `/sys`

- `/tmp`
- `/usr/*`
- `/usr/bin/`
- `/usr/local/*`
- `/usr/local/sbin/`
- `/usr/local/bin/`
- `/usr/sbin/`
- `/usr/lib/`
- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.

Файлы по указанным ниже путям доступны:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

3. В главном меню перейдите в раздел Мониторинг → Ресурсы и сервисы → **Активные сервисы** и установите флажок рядом с сервисом хранилища в зеленом статусе.

4. На панели инструментов или в меню (⋮) выберите **Резервное копирование** и нажмите **Создать резервную копию**.

   Параметр **Создать резервную копию** доступен, если выбран один сервис хранилища с зеленым статусом.

   Параметр недоступен при следующих условиях:

   - Если на предыдущем шаге вы установили флажок рядом с несколькими сервисами.
   - Если сервис хранилища имеет красный статус.
   - Если не установлен ни один флажок.
   - Если вы установили флажок рядом с другим типом сервиса.

5. В открывшемся окне **Резервное копирование партиций** настройте следующие параметры:

   a. В раскрывающемся списке **Тенант** выберите тенант, в котором находится партиция для резервного копирования.

   b. В раскрывающемся списке **Пространства** выберите одно или несколько пространств хранилища, которые принадлежат партиции для резервного копирования. Если значение не указано, будет выполнено резервное копирование партиции целиком.

   c. В раскрывающемся списке **Реплики** выберите одну или все реплики, для которых следует выполнить резервное копирование. При выборе нескольких реплик одного шарда произойдет дублирование данных.

   d. В поле **Диапазон дат** укажите с помощью календаря диапазон дат для партиций, которые войдут в резервную копию.

6. Нажмите **OK**.

7. В открывшемся окне подтверждения **Будет произведена процедура резервного копирования** нажмите **OK**.

   После подтверждения настройки параметров в разделе **Диспетчер задач** будет создана задача резервного копирования партиций и событие аудита.

Резервное копирование вручную выполнено.

После сохранения параметров по указанному пути будет автоматически созданы директории **backup** и **restore**. В директории **backup** будут автоматически созданы вложенные директории с идентификатором тенанта и идентификатором пространства. Например, если вы указали путь хранения резервной копии /mnt/data, полный путь к файлу резервной копии будет выглядеть следующим образом: /mnt/data/backup/<идентификатор тенанта>/<идентификатор пространства хранилища>/<дата создания партиции>.zip. Если вам необходимо узнать идентификатор тенанта или пространства, вы можете перейти в раздел **События**, открыть карточку события и просмотреть информацию.

Для восстановления из резервной копии необходимо будет перенести файл резервной копии в директорию **restore**.

Если имя файла при резервном копировании вручную совпало с именем файла резервной копии по расписанию, возвращается ошибка о невозможности сохранить файл резервной копии. Необходимо переименовать файл или удалить файл и выполнить резервное копирование вручную еще раз.

Об ошибке выполнения резервного копирования можно узнать в разделе **Активные сервисы** из желтого статуса сервиса хранилища и сообщения об ошибке, в разделе **Диспетчер задач** или событие аудита.

Импорт партиций из стороннего экземпляра OSMP

Импорт партиций из стороннего экземпляра OSMP доступен пользователям с ролью Главный администратор.

Чтобы выполнить импорт партиций из стороннего экземпляра OSMP:

1. Выдайте пользователю kuma права доступа к директории хранения резервной копии, которую вы указывали при настройке параметров резервного копирования, а также права доступа к файлу резервной копии с помощью следующих команд:

```
sudo chown kuma <полный путь к директории хранения резервной копии>
sudo chown kuma *.zip
```

2. Поместите файл для импорта партиций в директорию **restore**. Из этой директории будет выполняться импорт партиций.

3. В главном меню приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом хранилища, который имеет зеленый статус.

4. На панели инструментов или в меню (⋮) выберите **Резервное копирование** → **Импортировать**.

5. В появившемся окне **Импорт из стороннего экземпляра OSMP** настройте следующие параметры:

   a. В раскрывающемся списке **Тенант** выберите тенант, для которого будет выполняться импорт партиций.

   b. В раскрывающемся списке **Реплики** выберите одну реплику, в которую будут импортированы партиции.

   c. В раскрывающемся списке **Поля для исключений** укажите поля, которые необходимо удалить при импорте, установив или сняв флажки.

      По умолчанию установлены флажки для следующих полей:

      - AggregationRuleName.
      - CorrelationRuleName.
      - SourceAccountID.
      - DestinationAccountID.
      - SourceAssetID.
      - DestinationAssetID.
      - DeviceAssetID.
      - Поля расширенной схемы событий KUMA:
        - Поля расширенной схемы событий.
        - Поля активов KSC.
        - KLCorrelationRulePriority = "KL_CorrelationRulePriority"
        - KLSourceAssetDisplayName = "KL_SourceAssetDisplayName"
        - KLDestinationAssetDisplayName = "KL_DestinationAssetDisplayName"
        - KLDeviceAssetDisplayName = "KL_DeviceAssetDisplayName"
        - KLSourceAccountDisplayName = "KL_SourceAccountDisplayName"
        - KLDestinationAccountDisplayName = "KL_DestinationAccountDisplayName"

- KLDllHijackingResult = "KL_AI_DLLHijackingCheckResult"

  При выборе для удаления категории **Поля расширенной схемы событий KUMA** происходит удаление всей группы полей. Невозможно удалить только какую-то часть полей.

По умолчанию следующие поля будут удалены и поэтому недоступны для выбора в веб-интерфейсе:

- ServiceID.
- ServiceName.
- CorrelationRuleID.
- AggregationRuleID.

6. Нажмите **OK**.
7. В открывшемся окне подтверждения **Будет произведена процедура импорта** нажмите **OK**.

   После подтверждения настройки параметров в разделе **Диспетчер задач** будет создана задача импорта партиций и событие аудита.

Импорт партиции из стороннего экземпляра OSMP выполнен.

Восстановление партиций из резервной копии

Восстановление партиций из резервной копии доступно только пользователям с ролью Главный администратор.

Чтобы выполнить восстановление партиции из резервной копии:

1. Выдайте пользователю kuma права доступа к директории хранения резервной копии, которую вы указывали при настройке параметров резервного копирования, а также права доступа к файлу резервной копии с помощью следующих команд:

   ```
   sudo chown kuma <полный путь к директории хранения резервной копии>
   sudo chown kuma *.zip
   ```

2. Перенесите файл резервной копии из директории **backup** в директорию **restore**.
3. В главном меню перейдите в раздел Мониторинг → Ресурсы и сервисы → **Активные сервисы** и установите флажок рядом с сервисом хранилища в зеленом статусе.
4. На панели инструментов или в меню (⋮) выберите **Резервное копирование** → **Восстановить**.
5. В открывшемся окне **Восстановление из текущей установки KUMA** в раскрывающемся списке **Реплики** выберите одну реплику, в которой будет выполнено восстановление из резервной копии.
6. Нажмите **OK**.
7. В открывшемся окне подтверждения **Будет произведена процедура восстановления** нажмите **OK**.

   После подтверждения настройки параметров в разделе **Диспетчер задач** будет создана задача восстановления партиций из резервной копии и событие аудита.

Восстановление партиций из резервной копии выполнено.

Создание коллектора

Коллектор состоит из двух частей: одна часть создается внутри OSMP, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий.

Действия в Консоли KUMA

Коллектор создается в Консоли OSMP с помощью мастера установки. Этот мастер объединяет необходимые ресурсы в набор ресурсов для коллектора. После завершения работы мастера на основе этого набора ресурсов автоматически создается сам сервис.

Чтобы создать коллектор в Консоли OSMP,

Запустите мастер установки коллектора:

- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** нажмите **Подключить источник**.
- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** → **Коллекторы** нажмите **Добавить коллектор**.

В результате выполнения шагов мастера в Консоли OSMP создается сервис коллектора.

В набор ресурсов для коллектора объединяются следующие ресурсы:

- коннектор;
- нормализатор (как минимум один);
- фильтры (при необходимости);
- правила агрегации (при необходимости);
- правила обогащения (при необходимости);
- точки назначения (как правило, две: задается отправка событий в коррелятор и хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коллектора OSMP

При установке коллектора на сервер, предназначенный для получения событий, требуется запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в OSMP, а также используемый для связи порт.

Проверка установки

После создания коллектора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коллектора

Коллектор состоит из двух частей: одна часть создается внутри Консоли OSMP, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий. В мастере установки создается первая часть коллектора.

Чтобы запустить мастер установки коллектора:

- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** нажмите **Подключить источник**.
- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** → **Коллекторы** нажмите **Добавить коллектор**.

Следуйте далее указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

После завершения мастера в OSMP в разделе **Ресурсы и сервисы** → **Коллекторы** создается набор ресурсов для коллектора, а в разделе **Ресурсы и сервисы** → **Активные сервисы** добавляется сервис коллектора.

Шаг 1. Подключение источников событий

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коллектора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коллектора:

1. В поле **Название коллектора** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

   При создании некоторых типов коллекторов вместе с ними автоматически создаются агенты, имеющие название "agent: <Название коллектора>, auto created". Если такой агент уже создавался ранее и не был удален, то коллектор с названием <Название коллектора> невозможно будет создать. В такой ситуации необходимо или указать другое название коллектора, или удалить ранее созданный агент.

2. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коллектор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

   Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в службу. В службе можно добавлять только ресурсы из выбранного и общего тенантов.

3. В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать службу. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлена служба.

4. При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.

   Сообщения об ошибках сервиса коллектора помещаются в журнал, даже если режим отладки выключен. Журнал можно просмотреть на машине, где установлен коллектор, в директории /opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector.

5. В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

Основные параметры коллектора будут заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Транспорт

Это обязательный шаг мастера установки. На вкладке мастера установки **Транспорт** следует выбрать или создать коннектор, в параметрах которого будет определено, откуда сервис коллектора должен получать события.

Чтобы добавить в набор ресурсов существующий коннектор,

выберите в раскрывающемся списке **Коннектор** название нужного коннектора.

На вкладке мастера установки **Транспорт** отобразятся параметры выбранного коннектора. Выбранный коннектор можно открыть для редактирования в новой вкладке браузера с помощью кнопки ↗.

Для корректной работы предустановленного коллектора **[OOTB] Kaspersky EDR** параметр **Режим TLS** в свойствах указанного вами коннектора должен иметь значение **Включено**.

Чтобы создать коннектор:

1. Выберите в раскрывающемся списке **Коннектор** пункт **Создать**.

2. В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:

   - tcp
   - udp
   - netflow
   - sflow

- nats-jetstream
- kafka
- http
- sql
- file
- ftp
- nfs
- wmi
- wec
- snmp

При использовании типа коннектора **tcp** или **udp** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса активов, с которых были получены события.

При использовании типа коннектора **wmi** или **wec** будут автоматически созданы агенты для приема событий Windows.

Рекомендуется использовать кодировку по умолчанию (то есть UTF-8) и применять другие параметры только при получении в полях событий битых символов.

> Для настройки коллекторов OSMP на прослушивание портов с номерами меньше 1000 сервис нужного коллектора необходимо запускать с правами root. Для этого после установки коллектора в его конфигурационный файл systemd в раздел [Service] требуется дописать строку `AmbientCapabilities=CAP_NET_BIND_SERVICE`.
> Systemd-файл располагается в директории /usr/lib/systemd/system/kuma-collector-<`идентификатор коллектора`>.service.

Коннектор добавлен в набор ресурсов коллектора. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы и сервисы** → **Коннекторы**.

Перейдите к следующему шагу мастера установки.

Шаг 3. Парсинг событий

Это обязательный шаг мастера установки. На вкладке мастера установки **Парсинг событий** следует выбрать или создать нормализатор, в параметрах которого будут определены правила преобразования сырых событий в нормализованные. В нормализатор можно добавить несколько правил парсинга событий, реализуя таким образом сложную логику обработки событий. Вы можете протестировать работу нормализатора, используя тестовые события.

При создании нового нормализатора в мастере установки по умолчанию он будет сохранен в наборе ресурсов для коллектора и не сможет быть использован в других коллекторах. С помощью флажка **Сохранить нормализатор** вы можете создать нормализатор в виде отдельного ресурса, в таком случае нормализатор будет доступен для выбора в других коллекторах тенанта.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Добавление нормализатора

Чтобы добавить в набор ресурсов существующий нормализатор:

1. Нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора и активной вкладкой **Схема нормализации**.

2. В раскрывающемся списке **Нормализатор** выберите нужный нормализатор. В раскрывающемся списке доступны нормализаторы, принадлежащие тенанту коллектора и Общему тенанту.

   В окне **Основной парсинг событий** отобразятся параметры выбранного нормализатора.

   Если вы хотите отредактировать параметры нормализатора, в раскрывающемся списке **Нормализатор** нажмите на значок карандаша рядом с названием нужного нормализатора. Откроется окно **Редактирование нормализатора** с темным кружком. Если вы нажмете на темный кружок, откроется окно **Основной парсинг событий** и параметры нормализатора будут доступны для редактирования.

   Если вы хотите настроить параметры дополнительного парсинга, наведите курсор на темный кружок и нажмите на появившийся значок плюса, откроется окно **Дополнительный парсинг событий**. Подробнее о настройке расширенного анализа событий см. инструкцию ниже.

3. Нажмите на кнопку **OK**.

На вкладке мастера установки **Основной парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для просмотра.

Чтобы создать в коллекторе новый нормализатор:

1. На шаге Парсинг событий на вкладке **Схемы парсинга** нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора и активной вкладкой **Схема нормализации**.

2. Если хотите сохранить нормализатор в качестве отдельного ресурса, установите флажок **Сохранить нормализатор** - таким образом сохраненный нормализатор будет доступен для использования в других коллекторах тенанта. По умолчанию флажок снят.

3. Введите в поле **Название** уникальное имя для нормализатора. Название должно содержать от 1 до 128 символов Юникода.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требующие заполнения.

Доступный метод парсинга: json

Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

При обработке файлов с иерархически выстроенными данными можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы некорректно.

В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и, следовательно, в дополнительный нормализатор передается обрабатываемое событие целиком.

В качестве разделителя строк могут выступать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

5. В раскрывающемся списке **Сохранить сырое событие** укажите, надо ли сохранять сырое событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не сохранять** – не сохранять сырое событие. Это значение используется по умолчанию.

   - **При возникновении ошибок** – сохранять сырое событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке службы. В этом случае каждый раз, когда у события есть непустое поле `Raw`, это означает, что возникла проблема.

     > Если поля с названиями `*Address` или `*Date*` не соответствуют правилам нормализации, такие поля игнорируются. При этом не возникает ошибка нормализации и значения полей не попадают в поле `Raw` нормализованного события, даже если был указан параметр **Сохранить сырое событие** → **При возникновении ошибок**.

   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

6. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля сырого события в нормализованном событии, если для них не были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события `Extra`. Нормализованные события можно искать и фильтровать по данным, хранящимся в поле `Extra`.

   Фильтрация по данным из поля события Extra

   Условия для фильтров по данным из поля события **Extra**:

   - Условие – **Если**.

   - Левый операнд – **поле события**.

- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

По умолчанию поля не сохраняются.

7. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.
8. В таблице **Сопоставление** настройте сопоставление полей сырого события с полями событий в формате KUMA:

   a. В столбце **Исходные данные** укажите название поля сырого события, которое вы хотите преобразовать в поле события KUMA.

   Подробнее о формате полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

   Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором при нажатии на кнопку **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

   Доступные преобразования

   Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

   Доступные преобразования:

   - **lower** – используется для перевода всех символов значения в нижний регистр
   - **upper** – используется для перевода всех символов значения в верхний регистр
   - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⠿, а также удалять с помощью значка ×.

b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

Рекомендации для полей столбцов KUMA

Рекомендуется настроить сопоставление для следующих полей KUMA. Иначе вы не сможете просматривать наблюдаемые объекты в деталях алертов и инцидентов.

Рекомендуемые поля KUMA зависят от типов наблюдаемых объектов:

- Для наблюдаемых объектов типа MD5 и SHA256:
  - FileHash
- Для наблюдаемых объектов типа URL:
  - RequestUrl
- Для наблюдаемых объектов типа IP-адреса:
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress

- Для наблюдаемых объектов типа Доменное имя:
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain
  - SourceDnsDomain
  - SourceNtDomain
- Для наблюдаемых объектов типа UserName:
  - DestinationUserName
  - SourceUserName
- Для наблюдаемых объектов типа HostName:
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с `DeviceCustom*` и `Flex*`, в поле **Подпись** можно добавить уникальную пользовательскую метку.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

Чтобы KUMA могла выполнить обогащение событий данными про активы, и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам необходимо настроить сопоставление полей для адреса устройства и имени устройства в зависимости от назначения актива. Например, сопоставление для SourceAddress и SourceHostName, или DestinationAddress и DestinationHostName. В результате обогащения в карточке события появится поле SourceAssetID или DestinationAssetID и ссылка, по которой можно будет перейти в карточку актива. Также в результате обогащения сведения об активе будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля сырого события в поле события KUMA.

Если размер поля события KUMA оказывается меньше длины помещаемого в него значения, значение обрезается до размера поля события.

9. Нажмите на кнопку **OK**.

На вкладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Если вы хотите открыть параметры нормализатора для просмотра, нажмите на темный кружок. При наведении курсора мыши на кружок отображается знак плюса. Нажмите на значок "плюс", чтобы добавить правила парсинга событий (см. инструкцию ниже).

Обогащение нормализованного события дополнительными данными

В только что созданные нормализованные события можно добавлять дополнительные данные, создавая в нормализаторе правила обогащения. Эти правила хранятся в нормализаторе, в котором они были созданы. Правил обогащения может быть несколько.

Чтобы добавить правила обогащения в нормализатор:

1. Выберите основное или дополнительное правило нормализации, а затем в открывшемся окне перейдите на вкладку **Обогащение**.

2. Нажмите на кнопку **Добавить обогащение**.

   Появится блок параметров правила обогащения. Блок параметров можно удалить, нажав на кнопку ×.

3. В раскрывающемся списке **Тип источника** выберите тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые требуется заполнить.

   Доступные типы источников обогащения:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

   - **dictionary**

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

     Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

     Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

     Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбран тип **Событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом `Массив строк`, а целевым полем является поле с типом `Строка`, значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем `Массив строк` и целевое поле полем `Массив строк`, значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` — это название поля события, значение которого должно быть передано в скрипт.

    Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

   Этот параметр недоступен для типа источника обогащения **таблица**.

5. Если вы хотите включить детализацию в журнале нормализатора, переведите переключатель **Отладка** в активное положение. По умолчанию детализация отключена.

6. Нажмите на кнопку **OK**.

В нормализатор, в выбранное правило парсинга, добавлены правила обогащения событий дополнительными данными.

Настройка парсинга с привязкой к IP-адресам

Вы можете направить события с нескольких IP-адресов, от источников разных типов в один коллектор, и коллектор применит соответствующие заданные нормализаторы.

Такой способ доступен для коллекторов с коннектором типа UDP, TCP, HTTP. Если в коллекторе на шаге **Транспорт** указан коннектор UDP, TCP, HTTP, на шаге **Парсинг событий** на вкладке **Настройки парсинга** вы можете задать несколько IP-адресов и указать, какой нормализатор следует использовать для событий, поступающих с заданных адресов. Доступны следующие типы нормализаторов: json, cef, regexp, syslog, csv, kv, xml.

Если в коллекторе с настроенными нормализаторами с привязкой к IP-адресам вы измените тип коннектора на какой-либо, кроме UDP, TCP, HTTP, вкладка **Настройки парсинга** исчезнет и на шаге **Парсинг** будет указан только первый нормализатор из указанных прежде. Вкладка исчезает в веб-интерфейсе сразу, изменения будут применены после сохранения ресурса. Если вы хотите вернуться к прежним параметрам, выйдите из мастера установки коллектора без сохранения.

Для нормализаторов типа Syslog и regexp допускается использование цепочки нормализаторов: вы можете задать дополнительные условия нормализации в зависимости от значения поля DeviceProcessName. Отличие от дополнительной нормализации: вы можете указывать общедоступные нормализаторы.

Чтобы настроить парсинг с привязкой к IP-адресам:

1. На шаге **Парсинг событий** перейдите на вкладку **Настройки парсинга**.

2. В поле **IP-адрес(-а)** укажите один или несколько IP-адресов, с которых будут поступать события. Вы можете указать несколько IP-адресов через запятую. Доступный формат: IPv4. Длина списка адресов не ограничена, при этом рекомендуется указывать разумное количество адресов для соблюдения баланса нагрузки на коллектор. Поле обязательно для заполнения, если вы хотите применять несколько нормализаторов в одном коллекторе.

   Ограничение: IP-адрес должен быть уникальным для каждой комбинации IP + нормализатор. OSMP выполняет проверку уникальности адресов. Если вы укажете один и тот же IP-адрес для разных нормализаторов, отобразится сообщение **Поле должно быть уникальным**.

   Если вы планируете отправлять все события в один нормализатор без указания IP-адресов, рекомендуется создать отдельный коллектор. Также рекомендуется создать отдельный коллектор с одним нормализатором, если вы хотите применить один нормализатор к событиям с большого количества IP-адресов - в таком варианте производительность будет выше.

3. В поле **Нормализатор** создайте или выберите в раскрывающемся списке существующий нормализатор. Стрелка рядом с раскрывающимся списком позволяет выполнить переход на вкладку **Схемы парсинга**.

   Нормализация будет срабатывать если у вас настроен тип коннектора: UDP, TCP, HTTP, при этом для HTTP должен быть указан header источника событий.

   С учетом доступных коннекторов, следующие типы нормализатора доступны для автоматического распознавания источников: json, cef, regexp, syslog, csv, kv, xml.

4. Если вы выбрали тип нормализатора Syslog или regexp, вы можете **Добавить условную нормализацию**. Условная нормализация будет доступна, если в основном нормализаторе настроено **Сопоставление полей** для DeviceProcessName. В группе параметров **Условие** укажите имя процесса в поле DeviceProcessName и создайте или выберите из раскрывающегося списка существующий нормализатор. Вы можете указать несколько комбинаций DeviceProcessName + нормализатор, нормализация будет выполняться до первого совпадения.

Настройка парсинга с привязкой к IP-адресам выполнена.

Создание структуры правил нормализации событий

Для реализации сложной логики обработки событий в нормализатор можно добавить более одного правила парсинга событий. События передаются между правилами парсинга в зависимости от заданных условий. Последовательность создания правил парсинга важна. Событие обрабатывается последовательно, путь к нему отображается стрелками.

Чтобы создать дополнительное правило парсинга:

1. Создайте нормализатор (см. инструкцию выше).

   Созданный нормализатор отобразится в окне в виде темного кружка.

2. Наведите указатель мыши на кружок и нажмите на появившуюся кнопку со значком плюса.

3. В открывшемся окне **Дополнительный парсинг событий** задайте параметры дополнительного правила парсинга события:

   - Вкладка **Условия дополнительной нормализации**:

Если вы хотите передавать сырое событие для дополнительной нормализации, в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**. По умолчанию указано значение **Нет**. Рекомендуется передавать сырое событие в нормализаторы типа json и xml. Если вы хотите передавать сырое событие для дополнительной нормализации на второй, третий и далее уровень вложенности, последовательно на каждом уровне вложенности в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**.

Если вы хотите отправлять в дополнительный нормализатор только события с определенным полем, укажите его в поле **Поле, которое следует передать в нормализатор**.

На этой вкладке вы также можете определить другие условия. При выполнении этих условий событие отправляется на дополнительный анализ.

- Вкладка **Схема нормализации**:

  На этой вкладке можно настроить правила обработки событий, по аналогии с параметрами основного нормализатора (см. инструкцию выше). Параметр **Сохранить сырое событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании начального нормализатора.

- Вкладка **Обогащение**:

  На этой вкладке можно настроить правила обогащения событий (см. инструкцию выше).

4. Нажмите на кнопку **OK**.

Дополнительное правило парсинга добавлено в нормализатор и отображается в виде темного блока, на котором указаны условия, при котором это правило будет задействовано. Параметры дополнительного правила парсинга можно изменить, нажав на него. Если навести курсор мыши на правило дополнительного парсинга, отобразится кнопка с плюсом. Вы можете нажать на эту кнопку, чтобы создать дополнительное правило парсинга. С помощью кнопки со значком корзины нормализатор можно удалить.

В верхнем правом углу окна располагается окно поиска, где можно искать правила парсинга по названию.

Перейдите к следующему шагу мастера установки.

Шаг 4. Фильтрация событий

Это необязательный шаг мастера установки. На вкладке мастера установки **Фильтрация событий** можно выбрать или создать фильтр, в параметрах которого будут определены условия отбора событий. В коллектор можно добавить несколько фильтров. Фильтры можно менять местами, перетягивая их мышью за значок ⣿, и удалять. Фильтры объединены оператором И.

Чтобы добавить в набор ресурсов коллектора существующий фильтр,

Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите требуемый фильтр.

Чтобы добавить в набор ресурсов коллектора новый фильтр:

1. Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого фильтра. Название должно содержать от 1 до 128 символов Юникода.

4. В разделе **Условия** задайте условия, которым должны соответствовать отсеиваемые события:

- С помощью кнопки **Добавить условие** вы можете добавить условия фильтра. Вы можете выбрать два значения (два операнда, левый и правый) и назначить операцию, которую хотите выполнить с выбранными значениями. Результат операции – Истина (True) или Ложь (False).

  - В раскрывающемся списке **оператор** необходимо выбрать функцию, которую должен выполнять фильтр.

    В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

    Операторы фильтров

    - **=** – левый операнд равен правому операнду.
    - **<** – левый операнд меньше правого операнда.
    - **<=** – левый операнд меньше или равен правому операнду.
    - **>** – левый операнд больше правого операнда.
    - **>=** – левый операнд больше или равен правому операнду.
    - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
    - **contains** – левый операнд содержит значения правого операнда.
    - **startsWith** – левый операнд начинается с одного из значений правого операнда.
    - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
    - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
    - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

      Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

      Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
    - **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

      Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
    - **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
    - **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

- В раскрывающихся списках **Левый операнд** и **Правый операнд** необходимо выбрать, откуда поступят данные, с которыми произведет действие фильтр. Отобразятся дополнительные параметры. Используйте их, чтобы определить точное значение, которое будет передано фильтру. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.
- С помощью раскрывающегося списка **Если** можно выбрать, требуется ли создать отрицательное условие фильтра.

Условия можно удалить, нажав на кнопку ×.

- С помощью кнопки **Добавить группу** добавляются группы условий. Оператор **И** можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

  Группу условий можно удалить, нажав на кнопку ×.

- С помощью кнопки **Добавить фильтр** в условия добавляются существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**. В параметры вложенного фильтра можно перейти с помощью кнопки ↗.

  Вложенный фильтр можно удалить, нажав на кнопку ×.

Фильтр добавлен.

Перейдите к следующему шагу мастера установки.

Шаг 5. Агрегация событий

Это необязательный шаг мастера установки. На вкладке мастера установки **Агрегация событий** можно выбрать или создать правила агрегации, в параметрах которого будут определены условия для объединения однотипных событий. В коллектор можно добавить несколько правил агрегации.

Чтобы добавить в набор ресурсов коллектора существующее правило агрегации,

Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся списке выберите **Правило агрегации**.

Чтобы добавить в набор ресурсов коллектора новое правило агрегации:

1. Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся меню **Правило агрегации** выберите пункт **Создать**.

2. В поле **Название** введите название для создаваемого правила агрегации. Название должно содержать от 1 до 128 символов Юникода.

3. В поле **Предел событий** укажите количество событий, которое должно быть получено, чтобы сработало правило агрегации и события были объединены. По умолчанию указано значение `100`.

4. В поле **Время ожидания событий** укажите количество секунд, в течение которых коллектор получает события для объединения. По истечении этого срока правило агрегации срабатывает и создается новое агрегационное событие. По умолчанию указано значение `60`.

5. В разделе **Группирующие поля** нажмите на кнопку **Добавить поле** и выберите поля, по которым будут определяться однотипные события. Выбранные события можно удалить с помощью кнопок со значком крестика.

6. В разделе **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, при наличии которых коллектор исключит событие из процесса агрегации даже при наличии полей, указанных в разделе **Группирующие поля**. Выбранные события можно удалить с помощью кнопок со значком крестика.

7. В разделе **Поля суммы** нажмите на кнопку **Добавить поле** и выберите поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалить с помощью кнопок со значком крестика.

8. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

   Создание фильтра в ресурсах

   Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

   Операторы фильтров

   - **=** – левый операнд равен правому операнду.
   - **<** – левый операнд меньше правого операнда.
   - **<=** – левый операнд меньше или равен правому операнду.
   - **>** – левый операнд больше правого операнда.
   - **>=** – левый операнд больше или равен правому операнду.
   - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
   - **contains** – левый операнд содержит значения правого операнда.
   - **startsWith** – левый операнд начинается с одного из значений правого операнда.
   - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
   - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
   - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

     Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

     Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
   - **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

     Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
   - **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
   - **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.
6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Правило агрегации добавлено. Его можно удалить, нажав на кнопку ✕.

Перейдите к следующему шагу мастера установки.

Шаг 6. Обогащение события

Это необязательный шаг мастера установки. На вкладке мастера установки **Обогащение событий** можно указать, какими данными и из каких источников следует дополнить обрабатываемые коллектором события. События можно обогащать данными, полученными с помощью правил обогащения или с помощью LDAP.

Обогащение с помощью правил обогащения

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ✕. Можно использовать существующие правила обогащения или же создать правила непосредственно в мастере установки.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коллектора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

   - **dictionary**

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

     Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

     Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

     Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр
    - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
    - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
    - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
      - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
      - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
    - **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
    - **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.

- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.

- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

  Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то KUMA возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро KUMA.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.

Параметр	Описание
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

  Доступные параметры:

  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
  - **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.
  - **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

    Доступные типы индикаторов CyberTrace:

    - **ip**
    - **url**
    - **hash**

    В таблице сопоставления требуется указать как минимум одну строку. Нажав на кнопку **Добавить строку**, можно добавить строку, а на кнопку ✕ – удалить.

- **часовой пояс**

  Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере службы, использующей обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлена служба (коллектор или коррелятор), обрабатывающая событие. При изменении времени сервера службу необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- **геоданные;**

  Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

  При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

  1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

     С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

     > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. Можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события, нажав эту кнопку.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.

   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

   Создание фильтра в ресурсах

   Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

      a. Нажмите на кнопку **Добавить условие**.

      b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

      c. В раскрывающемся списке **Оператор** выберите оператор.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

В набор ресурсов для коллектора добавлено новое правило обогащения.

Обогащение с помощью LDAP

Чтобы включить обогащение с помощью LDAP:

1. Нажмите **Добавить сопоставление с учетными записями LDAP**.

   Откроется блок параметров обогащения с помощью LDAP.

2. В блоке параметров **Сопоставление с учетными записями LDAP** с помощью кнопки **Добавить домен** укажите домен учетных записей. Доменов можно указать несколько.

3. В таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP:

   - В столбце **Поле KUMA** укажите поле события KUMA, данные из которого следует сравнить с атрибутом LDAP.
   - В столбце **LDAP-атрибут**, укажите атрибут, с которым необходимо сравнить поле события KUMA. Раскрывающийся список содержит стандартные атрибуты и может быть дополнен **пользовательскими атрибутами**.

     Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

     Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

     1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

        Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартный атрибут `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

Из Active Directory можно запросить следующие атрибуты учетных записей:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `co`
- `company`
- `department`
- `description`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `givenName`
- `l`
- `lastLogon`
- `lastLogonTimestamp`
- `Mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSID`
- `physicalDeliveryOfficeName`

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

После того как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если вы добавили один и тот же атрибут для нескольких доменов, атрибут отображается в раскрывающемся списке только один раз. Вы можете просмотреть домены, наведя курсор на вопросительный знак. Названия доменов отображаются в виде ссылок. Если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

   После перезапуска коллектора KUMA начнет обогащать события учетными записями.

- В столбце **Поле для записи данных** укажите, в какое поле события KUMA следует поместить идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление было успешно.

С помощью кнопки **Добавить строку** в таблицу можно добавить строку, а с помощью кнопки ✕ – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

В блок ресурсов для коллектора добавлены правила обогащения события данными, полученными из LDAP.

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров

обогащения требуется остановить и запустить службу снова.

Перейдите к следующему шагу мастера установки.

Шаг 7. Маршрутизация

Это необязательный шаг мастера установки. На вкладке мастера установки **Маршрутизация** можно выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять обработанные коллектором события. Обычно события от коллектора перенаправляются в две точки: в коррелятор для анализа и поиска угроз; в хранилище для хранения, а также чтобы обработанные события можно было просматривать позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коллектора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Параметры точки назначения можно открыть для редактирования в новой вкладке браузера с помощью кнопки ↗.

3. Нажмите на кнопку **Сохранить**.

Выбранная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коллектора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.

- Выберите **Другое**, если хотите отправлять события в другие места.

  К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры на вкладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
     - Выберите **nats-jetstream**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats-jetstream**, **file** и **diode** с помощью кнопки **URL** можно указать несколько адресов отправки.
   - Для типов **nats-jetstream** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать символы Юникода. Топик для Kafka имеет ограничение длины в 255 символов.

3. При необходимости укажите параметры на вкладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора прокси-сервера.
   - **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. По умолчанию указано значение `30`.
   - **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
   - **Идентификатор кластера** – идентификатор кластера NATS.

- **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации.

  - **С проверкой** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. По умолчанию указано значение `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

  Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**.

  Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

  Создание фильтра в ресурсах

  Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

  Чтобы создать фильтр:

  1. В раскрывающемся списке **Фильтр** выберите **Создать**.

  2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

  3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

  4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

     a. Нажмите на кнопку **Добавить условие**.

     b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **Оператор** выберите оператор.

     Операторы фильтров

     - **=** – левый операнд равен правому операнду.
     - **<** – левый операнд меньше правого операнда.
     - **<=** – левый операнд меньше или равен правому операнду.
     - **>** – левый операнд больше правого операнда.
     - **>=** – левый операнд больше или равен правому операнду.
     - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
     - **contains** – левый операнд содержит значения правого операнда.
     - **startsWith** – левый операнд начинается с одного из значений правого операнда.
     - **endsWith** – левый операнд заканчивается одним из значений правого операнда.

- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.

- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

4. Нажмите на кнопку **Сохранить**.

   Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 8. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в OSMP создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коллектора отображается в разделе **Ресурсы и сервисы** → **Коллекторы**. Его можно использовать для создания новых служб коллектора. При изменении этого набора ресурсов все службы, работающие на основе этого набора ресурсов, начнут использовать новые параметры после перезапуска служб. Для этого вы можете использовать кнопки **Сохранить и перезапустить службы** и **Сохранить и обновить конфигурации служб**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы и сервисы** → **Активные сервисы**. Сервисы, созданные с помощью мастера установки, выполняют функции внутри OSMP. Чтобы взаимодействовать с внешними частями сетевой инфраструктуры, вам необходимо установить аналогичные внешние службы на предназначенные для них серверы и активы. Например, внешнюю службу коллектора следует установить на сервере, предназначенном для получения событий; внешние службы хранилища – на серверах с развернутой службой ClickHouse; внешние службы агентов – на тех активах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите на кнопку **Создать и сохранить службу**.

   На вкладке мастера установки **Проверка параметров** отображается таблица служб, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих служб на предназначенные для них серверы и активы.

   Например:

   ```
   /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
   ```

   где:

   - <FQDN> – полное доменное имя сервера Ядра KUMA.
   - <port> – порт, используемый для связи с Ядром KUMA.
   - <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

     Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор отпечатка сертификата центра сертификации Ядра KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также вам нужно убедиться в сетевом подключении OSMP и при необходимости открыть используемые компонентами OSMP порты.

2. Закройте мастер, нажав **Сохранить коллектор**.

Сервис коллектора создан в OSMP. Теперь аналогичную службу необходимо установить на сервере, предназначенном для получения событий.

Если в коллекторы был выбран коннектор типа wmi или wec, потребуется также установить автоматически созданные агенты OSMP.

Установка коллектора в сетевой инфраструктуре KUMA

Коллектор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий. В сетевой инфраструктуре устанавливается вторая часть коллектора.

Чтобы установить коллектор:

1. Войдите на сервер, на котором вы хотите установить службу.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска. Если файл не является исполняемым, измените права для запуска с помощью следующей команды:

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```

4. Поместите в директорию /opt/kaspersky/kuma/ файл LICENSE из /kuma-ansible-installer/roles/kuma/files/ и примите условия Лицензионного соглашения, выполнив следующую команду:

```
sudo /opt/kaspersky/kuma/kuma license
```

5. Создайте пользователя kuma:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

6. Выдайте пользователю kuma права на директорию /opt/kaspersky/kuma и все файлы внутри директории:

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

7. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA
Core CA certificate> --id <service ID> --api.port <API port>
```

где:

- <FQDN> – полное доменное имя сервера Ядра KUMA.
- <port> – порт, используемый для связи с Ядром KUMA.
- <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

  Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

  Для обеспечения проверки подлинности CA-сертификата Ядра KUMA рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.
- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

Пример:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
--api.port YYYY
```

Если в результате выполнения команды были выявлены ошибки, проверьте корректность параметров. Например, наличие требуемого уровня доступа, сетевой доступности между службой коллектора и ядром, уникальность выбранного API-порта. После устранения ошибок продолжите установку коллектора.

Если ошибки не выявлены, а статус коллектора в Консоли KUMA изменился на *зеленый*, остановите выполнение команды и перейдите к следующему шагу.

Команду можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коллектора, а также порт, который этот коллектор использует для связи.

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

8. Выполните команду повторно, добавив ключ `--install`:

```
sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA
Core CA certificate> --id <service ID> --api.port <API port> --install
```

где:

- <FQDN> – полное доменное имя сервера Ядра KUMA.
- <port> – порт, используемый для связи с Ядром KUMA (по умолчанию используется порт 7210).
- <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

  Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

  Для обеспечения проверки подлинности CA-сертификата Ядра KUMA рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.
- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

Пример:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
--api.port YYYY --install
```

9. Добавьте порт коллектора KUMA в исключения брандмауэра.

> Для правильной работы приложения убедитесь, что компоненты KUMA могут взаимодействовать с другими компонентами и приложениями по сети через протоколы и порты, указанные во время установки компонентов KUMA.

Коллектор установлен. С его помощью можно получать и передавать на обработку данные из источника события.

Проверка правильности установки коллектора

Проверить готовность коллектора к получению событий можно следующим образом:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Активные сервисы**.

2. Убедитесь, что у установленного вами коллектора зеленый статус.

   Если статус коллектора отличается от зеленого, просмотрите журнал этой службы на машине, где она установлена, в директории /opt/kaspersky/kuma/collector/<идентификатор корректора>/log/collector. Ошибки записываются в журнал вне зависимости от того, включен или выключен режим отладки.

Если коллектор установлен правильно и вы уверены, что из источника событий приходят данные, то при поиске связанных с ним событий в таблице должны отображаться события.

*Чтобы проверить наличие ошибок нормализации с помощью раздела **События** Консоли KUMA:*

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в KUMA.

3. Убедитесь, что в разделе **Ресурсы** Консоли KUMA в раскрывающемся списке **Хранить сырое событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.

4. В разделе **События** в KUMA выполните поиск событий со следующими параметрами:

   - `ServiceID = <идентификатор коллектора, который требуется проверить>`

   - `Raw != ""`

   Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana™:

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в KUMA.

3. Откройте раздел Метрики и перейдите по ссылке KUMA Collectors.

4. Проверьте, отображаются ли ошибки в разделе Errors (Ошибки) виджета Normalization (Нормализация).

   Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

В коллекторах типа WEC и WMI необходимо убедиться, что для подключения к агенту используется уникальный порт. Этот порт указывается в разделе **Транспорт** мастера установки коллектора.

Обеспечение бесперебойной работы коллекторов

Бесперебойное поступление событий от источника событий в KUMA является важным условием защиты сетевой инфраструктуры. Бесперебойность можно обеспечить автоматическим перенаправлением потока событий на большее число коллекторов:

- На стороне KUMA необходимо установить два или больше одинаковых коллекторов.
- На стороне источника событий необходимо настроить управление потоками событий между коллекторами с помощью сторонних средств управления нагрузкой серверов, например rsyslog или nginx.

При такой конфигурации коллекторов поступающие события не будут теряться, когда сервер коллектора по какой-либо причине недоступен.

Необходимо учитывать, что при переключении потока событий между коллекторами агрегация событий будет происходить на каждом коллекторе отдельно.

Если коллектор KUMA не удается запустить, а в его журнале выявлена ошибка "panic: runtime error: slice bounds out of range [8:0]":

1. Остановите коллектор.

   ```
   sudo systemctl stop kuma-collector-<идентификатор коллектора>
   ```

2. Удалите файлы с кешем DNS-обогащения.

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<идентификатор
   коллектора>/cache/enrichment/DNS-*
   ```

3. Удалите файлы с кешем событий (дисковый буфер). Выполняйте команду, только если можно пожертвовать событиями, находящимися в дисковых буферах коллектора.

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<идентификатор коллектора>/buffers/*
   ```

4. Запустите службу коллектора.

   ```
   sudo systemctl start kuma-collector-<идентификатор коллектора>
   ```

Управление потоком событий с помощью rsyslog

Чтобы включить управление потоками событий на сервере источника событий с помощью rsyslog:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.

2. Установите на сервере источника событий rsyslog (см. документацию rsyslog).

3. Добавьте в конфигурационный файл /etc/rsyslog.conf правила перенаправления потока событий между коллекторами:

```
*.* @@<FQDN основного сервера коллектора>:<порт, на который коллектор принимает события>
$ActionExecOnlyWhenPreviousIsSuspended on
& @@<FQDN резервного сервера коллектора>:<порт, на который коллектор принимает события>
$ActionExecOnlyWhenPreviousIsSuspended off
```

Пример конфигурационного файла

Пример конфигурационного файла, где указан один основной коллектор и два резервных. Коллекторы настроены на принятие событий на порт TCP 5140.

```
*.* @@kuma-collector-01.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended on
& @@kuma-collector-02.example.com:5140
& @@kuma-collector-03.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended off
```

4. Перезапустите rsyslog, выполнив команду:

   `systemctl restart rsyslog`.

Управление потоками событий на сервере источника событий включено.

Управление потоком событий с помощью nginx

Для управления потоком событий средствами nginx необходимо создать и настроить ngnix-сервер, который будет принимать события от источника событий, а затем перенаправлять их на коллекторы.

Чтобы включить управление потоками событий на сервере источника событий с помощью nginx:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.

2. Установите nginx на сервере, предназначенном для управления потоком событий.

   - Команда для установки в Oracle Linux 8.6:

     `$sudo dnf install nginx`

   - Команда для установки в Ubuntu 20.4:

     `$sudo apt-get install nginx`

     При установке из sources, необходимо собрать с параметром `-with-stream`:
     `$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

3. На nginx-сервере в конфигурационный файл nginx.conf добавьте модуль stream с правилами перенаправления потока событий между коллекторами.

   Пример модуля stream

Пример модуля, в котором поток событий распределяется между коллекторами kuma-collector-01.example.com и kuma-collector-02.example.com, которые принимают события по протоколу TCP на порт 5140 и по протоколу UDP на порт 5141. Для балансировки используется ngnix-сервер nginx.example.com.

```
stream {
 upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
 server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
 worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile is the limit on the number of open files (RLIMIT_NOFILE) for workers. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections is the maximum number of connections that a worker can open simultaneously.
```

4. Перезапустите nginx, выполнив команду:

   ```
   systemctl restart nginx
   ```

5. На сервере источника событий перенаправьте события на ngnix-сервер.

Управление потоками событий на сервере источника событий включено.

Для тонкой настройки балансировки может потребоваться nginx Plus, однако некоторые методы балансировки, например Round Robin и Least Connections, доступны в базовой версии ngnix.

Подробнее о настройке nginx см. в документации nginx.

Предустановленные коллекторы

В поставку OSMP включены перечисленные в таблице ниже предустановленные коллекторы.

Если вам нужно адаптировать предустановленный OOTB-ресурс к инфраструктуре своей организации, воспользуйтесь операцией дублирования. Также вы можете экспортировать и импортировать ресурсы. Создание копии предустановленного ресурса вручную не гарантирует его работоспособность.

Имя	Описание
[OOTB] CEF	Собирает события в формате CEF, поступающие по протоколу TCP.
[OOTB] Kaspersky EDR	Собирает события от Kaspersky Endpoint Detection and Response в формате JSON.
[OOTB] KSC	Собирает события от Kaspersky Security Center по протоколу Syslog TCP.
[OOTB] KSC SQL	Собирает события от Kaspersky Security Center с использование запроса к базе данных MS SQL.
[OOTB] Syslog	Собирает события по протоколу Syslog.
[OOTB] Syslog-CEF	Собирает события в формате CEF, поступающих по протоколу UDP и имеющих заголовок Syslog.

Создание коррелятора

Коррелятор состоит из двух частей: одна часть создается внутри Консоли OSMP, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий.

Действия в Консоли OSMP

Коррелятор создается в Консоли OSMP с помощью мастера установки. Этот мастер объединяет необходимые ресурсы в набор ресурсов для коррелятора. После завершении работы мастера на основе этого набора ресурсов автоматически создается сам сервис.

Чтобы создать коллектор в OSMP,

запустите мастер установки коррелятора:

- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** нажмите **Создать коррелятор**.
- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** → **Корреляторы** нажмите **Создать коррелятор**.

В результате выполнения шагов мастера в OSMP создается сервис коррелятора.

В набор ресурсов для коррелятора объединяются следующие ресурсы:

- правила корреляции;
- правила обогащения (при необходимости);
- правила реагирования (при необходимости);
- точки назначения (как правило, одна: задается отправка событий в хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коррелятора OSMP

При установке коррелятора на сервер, предназначенный для обработки событий, на сервере требуется запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в OSMP, а также используемый для связи порт.

Проверка установки

После создания коррелятора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коррелятора

Чтобы запустить мастер установки коррелятора:

- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** нажмите **Создать коррелятор**.
- В главном меню Консоли OSMP в разделе **Ресурсы и сервисы** → **Корреляторы** нажмите **Создать коррелятор**.

Следуйте далее указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

После завершения мастера в OSMP в разделе **Ресурсы и сервисы** → **Корреляторы** создается набор ресурсов для коррелятора, а в разделе **Ресурсы и сервисы** → **Активные сервисы** добавляется сервис коррелятора.

Шаг 1. Общие параметры коррелятора

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коррелятора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коррелятора:

- В поле **Название** введите уникальное имя создаваемой службы. Название должно содержать от 1 до 128 символов Юникода.
- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коррелятор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

> Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в службу. В службе можно добавлять только ресурсы из выбранного и общего тенантов.

- В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать службу. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлена служба.

- При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.

- В поле **Описание** можно добавить описание службы: до 256 символов Юникода.

Основные параметры коррелятора заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Глобальные переменные

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными переменными. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменным можно присвоить какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Чтобы добавить глобальную переменную в корреляторе,

Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

- В окне **Переменная** введите название переменной.

  Требования к наименованию переменных

  - Должно быть уникально в рамках коррелятора.
  - Имя должно содержать от 1 до 128 символов Юникода.
  - Не может начинаться с символа $.
  - Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  Описание функций переменных.

Глобальная переменная добавлена. К ней можно обращаться из правил корреляции, добавляя перед названием переменной символ $. Переменных может быть несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Перейдите к следующему шагу мастера установки.

Шаг 3. Корреляция

Это необязательный, но рекомендуемый шаг мастера установки. На вкладке мастера установки **Корреляция** следует выбрать или создать правила корреляции. Эти ресурсы определяют последовательность событий, которые указывают на инциденты, связанные с безопасностью. При обнаружении этих последовательностей коррелятор создает событие корреляции и алерт.

Если вы добавили в коррелятор глобальные переменные, все добавленные правила корреляции могут к ним обращаться.

Добавленные в набор ресурсов для коррелятора правила корреляции отображаются в таблице со следующими столбцами:

- **Правила корреляции** – название ресурса правила корреляции.
- **Тип** – тип правила корреляции: **standard**, **simple**, **operational**. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.
- **Действия** – перечень действий, которые совершит коррелятор при срабатывании правила корреляции. Действия указываются в параметрах правила корреляции. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.

  Доступные значения:

  - **В дальнейшую обработку** – корреляционные события, создаваемые этим правилом корреляции, передается в другие ресурсы коррелятора: в обогащение, в правиле реагирования, а затем в другие сервисы OSMP.
  - **Изменение активного листа** – правило корреляции вносит изменения в активные листы.
  - **В коррелятор** – корреляционное событие отправляется на повторную обработку в то же правило корреляции.
  - **Изменение категорий** – корреляционное правило изменяет категории активов.
  - **Обогащение событий** – в корреляционном правиле настроено обогащение корреляционных событий.
  - **Не создавать алерт** – когда в результате срабатывания правила корреляции создается корреляционное событие, одновременно с ним НЕ создается алерт. Если вы не хотите создавать алерт при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Не создавать алерт**. Если вы установите только флажок **Не создавать алерт**, событие корреляции не сохраняется в хранилище.
  - **Общий ресурс** – правило корреляции или ресурсы, которые задействованы в правиле корреляции, расположены в общем тенанте.

С помощью поля **Поиск** можно искать правила корреляции. Добавленные правила корреляции можно убрать из набора ресурсов, выбрав нужные правила и нажав **Удалить**.

При выборе правила корреляции открывается окно с его параметрами: параметры можно изменить и **Сохранить**. При нажатии в этом окне на кнопку **Удалить**, правило корреляции отвязывается от набора ресурсов.

Используйте кнопки **Вверх** и **Вниз**, чтобы изменить положение выбранных правил корреляции в таблице. Это влияет на последовательность их выполнения при обработке событий. С помощью кнопки **Поднять operational-правила** можно переместить правила корреляции типа **operational** в начало списка правил корреляции.

Чтобы привязать к набору ресурсов для коррелятора существующие правила корреляции:

1. Нажмите **Привязать**.

   Откроется окно выбора ресурсов.

2. Выберите нужные правила корреляции и нажмите **OK**.

Правила корреляции привязаны к набору ресурсов для коррелятора и отображаются в таблице правил.

Чтобы создать в наборе ресурсов для коррелятора новое правило корреляции:

1. Нажмите на кнопку **Добавить**.

   Откроется окно создания правила корреляции.

2. Укажите параметры правила корреляции и нажмите **Сохранить**.

Правило корреляции создано и привязано к набору ресурсов для коррелятора. Оно отображается в таблице правил корреляции, а также в списке ресурсов в разделе **Ресурсы** → **Правила корреляции**.

Перейдите к следующему шагу мастера установки.

Шаг 4. Обогащение

Это необязательный шаг мастера установки. В вкладке мастера установки **Обогащение** можно выбрать или создать правила обогащения с указанием, какими данными и из каких источников следует дополнить создаваемые коррелятором корреляционные события. Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите на кнопку **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите на кнопку **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

- **dictionary**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

  Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

  Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

  Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

  Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

  Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.

  - В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр

    - **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` — это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

  Параметры этого типа обогащения описаны в таблице ниже.

  Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то KUMA возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро KUMA.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

  Доступные параметры:

  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.

  - **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.

- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.

- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - ip
  - url
  - hash

  В таблице сопоставления требуется указать как минимум одну строку. Нажав на кнопку **Добавить строку**, можно добавить строку, а на кнопку ✕ – удалить.

- **часовой пояс**

  Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

  При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

  > Убедитесь, что требуемый часовой пояс установлен на сервере службы, использующей обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

  При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

  По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлена служба (коллектор или коррелятор), обрабатывающая событие. При изменении времени сервера службу необходимо перезапустить.

  Допустимые форматы времени при обогащении поля DeviceTimeZone

  При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

   Создание фильтра в ресурсах

   Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

      a. Нажмите на кнопку **Добавить условие**.

      b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

      c. В раскрывающемся списке **Оператор** выберите оператор.

      Операторы фильтров

      - **=** – левый операнд равен правому операнду.
      - **<** – левый операнд меньше правого операнда.
      - **<=** – левый операнд меньше или равен правому операнду.
      - **>** – левый операнд больше правого операнда.
      - **>=** – левый операнд больше или равен правому операнду.
      - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
      - **contains** – левый операнд содержит значения правого операнда.

- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

В набор ресурсов для коррелятора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 5. Действие по реагированию

Это необязательный шаг мастера установки. На вкладке мастера установки **Реагирование** можно выбрать или создать правила реагирования с указанием, какие действия требуется выполнить при срабатывании правил корреляции. Правил реагирования может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

Чтобы добавить в набор ресурсов существующее правило реагирования:

1. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите нужный ресурс.

Правило реагирования добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило реагирования:

1. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите **Создать**.

3. В раскрывающемся списке **Тип** выберите тип правила реагирования и заполните относящиеся к нему параметры:

   - **Реагирование через KSC** – правила реагирования для автоматического запуска задач на активах Kaspersky Security Center. Например, вы можете настроить автоматический запуск антивирусной проверки или обновление базы данных.

     Автоматический запуск задач выполняется при интеграции OSMP с Kaspersky Security Center. Задачи запускаются только на активах, импортированных из Kaspersky Security Center.

     Параметры реагирования

     - **Задача Kaspersky Security Center** (обязательно) – название задачи Open Single Management Platform, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".

       Типы задач Open Single Management Platform, которые можно запустить с помощью KUMA:

       - Обновление.

       - Поиск вирусов.

- **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Open Single Management Platform. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

> Для отправки запросов в Open Single Management Platform необходимо убедиться, что Open Single Management Platform доступен по протоколу UDP.

- **Запуск скрипта** – правила реагирования для автоматического запуска скрипта. Например, вы можете создать скрипт с командами, которые требуется выполнить на сервере OSMP при обнаружении выбранных событий.

  Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts.

  Пользователю `kuma` этого сервера требуются права на запуск скрипта.

  Параметры реагирования

  - **Время ожидания** – количество секунд, которое выждет система, прежде чем запустить скрипт.
  - **Название скрипта** (обязательно) – имя файла скрипта.

    Если ресурс реагирования прикреплен к сервису коррелятора, однако в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
  - **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

    > Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

    Параметры можно обрамлять кавычками (").

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

    Пример: `-n "\"usr\": {{.SourceUserName}}"`

- **Реагирование через KEDR** – правила реагирования для автоматического создания правил запрета, запуска сетевой изоляции или запуска программы на активах Kaspersky Endpoint Detection and Response и Kaspersky Security Center.

  Автоматические действия по реагированию выполняются при интеграции OSMP с Kaspersky Endpoint Detection and Response.

Параметры реагирования

- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID
- **Тип задачи** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - Включить сетевую изоляцию.

    При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

    - **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов.

      При необходимости вы можете **добавить исключение для сетевой изоляции**.

      Чтобы добавить исключение для сетевой изоляции:

      a. Нажмите на кнопку **Добавить исключение**.

      b. Выберите направление сетевого трафика, которое не должно быть заблокировано:

      - Входящее.
      - Исходящее.
      - Входящее/Исходящее.

      c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.

      d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.

      e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.

      f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.

      > При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность приложения. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.

  - Выключить сетевую изоляцию.
  - Добавить правило запрета.

При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

- **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, запуск которых требуется запретить.

  Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в наследуемые поля правила корреляции.

- **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.

Хотя бы одно из указанных выше полей должно быть заполнено.

- Удалить правило запрета.
- Запустить приложение.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
  - **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
  - **Текущая директория** – директория, в которой на момент запуска располагается файл.

  При срабатывании правила реагирования для пользователей с ролью Главный администратор в разделе **Диспетчер задач** веб-интерфейса приложения отобразится задача **Запустить приложение**. В столбце **Создал** таблицы задач для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.

  Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск приложения.

  На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.

- **Реагирование через KICS for Networks** – правила реагирования для автоматического запуска задач в на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

  Автоматический запуск задач выполняется при интеграции OSMP с KICS for Networks.

  Параметры реагирования

  - **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
    - SourceAssetID
    - DestinationAssetID
    - DeviceAssetID

- **Задача KICS for Networks** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:

  - **Изменить статус актива на Разрешенное**.

  - **Изменить статус актива на Неразрешенное**.

  При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.

- **Реагирование через Active Directory** – правила реагирования для изменения прав пользователей Active Directory. Например, блокировать пользователя.

  Запуск задач выполняется при интеграции с Active Directory.

  Параметры реагирования

  - **Источник идентификатора аккаунта** – поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения:

    - SourceAccountID

    - DestinationAccountID

  - **Команда Active Directory** – команда, которая будет применяться к учетной записи при срабатывании правила реагирования. Доступные значения:

    - Добавить учетную запись в группу

    - Удалить учетную запись из группы

    - Сбросить пароль учетной записи

    - Блокировать учетную запись

- В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

  Поле не является обязательным.

1. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

   Создание фильтра в ресурсах

   Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

   Операторы фильтров

   - **=** – левый операнд равен правому операнду.
   - **<** – левый операнд меньше правого операнда.
   - **<=** – левый операнд меньше или равен правому операнду.
   - **>** – левый операнд больше правого операнда.
   - **>=** – левый операнд больше или равен правому операнду.
   - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
   - **contains** – левый операнд содержит значения правого операнда.
   - **startsWith** – левый операнд начинается с одного из значений правого операнда.
   - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
   - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
   - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

     Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

     Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку .

В набор ресурсов для коррелятора добавлено новое правило реагирования.

Перейдите к следующему шагу мастера установки.

Шаг 6. Маршрутизация

Это необязательный шаг мастера установки. На вкладке мастера установки **Маршрутизация** можно выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять созданные коррелятором события. Обычно события от коррелятора перенаправляются в хранилище для хранения и для возможности просматривать их позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коррелятора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки ↗.

3. Нажмите на кнопку **Сохранить**.

Выбранная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коррелятора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры на вкладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.

- Выберите **Тип** точки назначения:
  - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
  - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
  - Выберите **nats-jetstream**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
- Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

  Для всех типов, кроме **nats-jetstream** и **file**, с помощью кнопки **URL** можно указать несколько адресов отправки.
- Для типов **nats-jetstream** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать символы Юникода. Топик для Kafka имеет ограничение длины в 255 символов.

3. При необходимости укажите параметры на вкладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:
   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора прокси-сервера.
   - **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. По умолчанию указано значение `30`.
   - **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
   - **Идентификатор кластера** – идентификатор кластера NATS.
   - **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:
     - **Выключено** (по умолчанию) – не использовать шифрование TLS.
     - **Включено** – использовать шифрование, но без верификации.
     - **С проверкой** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

     При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. По умолчанию указано значение `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр.

  Создание фильтра в ресурсах

  Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

   Операторы фильтров

   - **=** – левый операнд равен правому операнду.
   - **<** – левый операнд меньше правого операнда.
   - **<=** – левый операнд меньше или равен правому операнду.
   - **>** – левый операнд больше правого операнда.
   - **>=** – левый операнд больше или равен правому операнду.
   - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
   - **contains** – левый операнд содержит значения правого операнда.
   - **startsWith** – левый операнд начинается с одного из значений правого операнда.
   - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
   - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
   - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

     Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

     Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

4. Нажмите на кнопку **Сохранить**.

Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 7. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в OSMP создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коррелятора отображается в разделе **Ресурсы** → **Корреляторы**. Его можно использовать для создания новой службы коррелятора. При изменении этого набора ресурсов все службы, работающие на основе этого набора ресурсов, начнут использовать новые параметры после перезапуска служб. Для этого вы можете использовать кнопки **Сохранить и перезапустить службы** и **Сохранить и обновить конфигурации служб**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Сервисы, созданные с помощью мастера установки, выполняют функции внутри OSMP. Чтобы взаимодействовать с внешними частями сетевой инфраструктуры, вам необходимо установить аналогичные внешние службы на предназначенные для них серверы и активы. Например, внешняя служба коррелятора следует установить на сервере, предназначенном для обработки событий; внешние службы хранилища – на серверах с развернутой службой ClickHouse; внешние службы агентов – на тех активах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите на кнопку **Создать и сохранить службу**.

   На вкладке мастера установки **Проверка параметров** отображается таблица служб, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих служб на предназначенные для них серверы и активы.

   Например:

   ```
   /opt/kaspersky/kuma/kuma correlator --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA
   certificate> --id <service ID> --api.port <API port> --install
   ```

   где:

   - <FQDN> – полное доменное имя сервера Ядра KUMA.
   - <port> – порт, используемый для связи с Ядром KUMA.
   - <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

     Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

     Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

     Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

> Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса, идентификатор отпечатка CA-сертификата Ядра KUMA и порт для связи с сервисом добавляются в команду автоматически. Также вам нужно убедиться в сетевом подключении OSMP и при необходимости открыть используемые компонентами OSMP порты.

2. Закройте мастер, нажав **Сохранить**.

Сервис коррелятора создан в OSMP. Теперь аналогичную службу необходимо установить на сервере, предназначенном для обработки событий.

Установка коррелятора в сетевой инфраструктуре OSMP

Коррелятор состоит из двух частей: одна часть создается внутри Консоли OSMP, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий. В сетевой инфраструктуре устанавливается вторая часть коррелятора.

Чтобы установить коррелятор:

1. Войдите на сервер, на котором вы хотите установить службу.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   > Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the
KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

где:

- <FQDN> – полное доменное имя сервера Ядра KUMA.
- <port> – порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)
- <fingerprint ID of the KUMA Core CA certificate> – идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Аргумент `--pair.fingerprint` является необязательным. При создании сервиса OSMP автоматически добавляет этот параметр в команду установщика и указывает идентификатор отпечатка.

Вы можете установить сервис без указания параметра `--pair.fingerprint`. В этом случае OSMP использует значение `insecure` по умолчанию, которое пропускает проверку сертификата центра сертификации (CA) Ядра KUMA при установлении подключения. Если значение `insecure`, отпечаток не нужно обновлять после перевыпуска сертификата центром сертификации (CA).

Чтобы убедиться, что сертификат центра сертификации (CA) Ядра KUMA прошел проверку, рекомендуется сохранить параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service ID> – это идентификатор сервиса KUMA, скопированный из веб-интерфейса.
- <API port> – это порт, используемый для связи с установленным компонентом.

Пример:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
--api.port YYYY --install
```

Команду, с помощью которой можно установить коррелятор на сервере, можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коррелятора, а также порт, который этот коррелятор использует для связи. Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Коррелятор установлен. С его помощью можно анализировать события на предмет угроз.

Проверка правильности установки коррелятора

Проверить готовность коррелятора к получению событий можно следующим образом:

1. В OSMP перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Убедитесь, что у установленного вами коррелятора зеленый статус.

Если в коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на вкладке событий будут отображаться события с параметрами `DeviceVendor=Kaspersky` и `DeviceProduct=KUMA`. Название сработавшего правила корреляции будет отображаться как название этих корреляционных событий.

Если корреляционные события не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте правило корреляции типа **simple** и одно действие **Отправить событие на дальнейшую обработку**. Рекомендуется создать фильтр для поиска событий, которые OSMP получает регулярно.

При обновлении, добавлении или удалении правила корреляции необходимо обновить конфигурацию коррелятора.

Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из OSMP и обновить параметры коррелятора.

Создание коррелятора correlator-ng

Коррелятор correlator-ng – это компонент OSMP, предназначенный для корреляции и обработки событий из различных источников. Он позволяет фильтровать, объединять и анализировать события с помощью правил корреляции, селекторов и выражений.

В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

В текущей версии коррелятор управляется только через YAML-конфигурацию. После первичного получения конфигурации от Ядра KUMA дальнейшее изменение параметров происходит напрямую в файлах, без возможности использовать веб-интерфейс OSMP для управления коррелятором.

Correlator-ng не является полностью совместимой заменой стандартной модели коррелятора.

Основные отличия:

- Новый синтаксис правил и селекторов, совместимый с SQL-подобными выражениями и функциями.
- Поддержка join-селекторов: события разных селекторов сравниваются параллельно в порядке их поступления.
- Возможность использования атрибута `anyMatch` для срабатывания правила корреляции, если хотя бы один селектор достиг своего порогового значения.
- Расширенный набор функций для работы с типами данных, массивами, строками, временными метками и CyberTrace-полями.
- Более строгая типизация выражений и автоматическое приведение значений полей и переменных к необходимому типу для правильного выполнения операций.
- Изменен синтаксис регулярных выражений: в correlator-ng используется синтаксис PCRE-like, а в стандартной модели коррелятора используется RE2.

Ограничения correlator-ng

У текущей реализации correlator-ng есть ряд ограничений:

- Коррелятор не может автоматически классифицировать активы на основе поступающих событий и не поддерживает действия, которые обычно выполняются при срабатывании правил реагирования.
- Коррелятор не может автоматически обогащать события дополнительными данными из внешних источников, таких как DNS-запросы, скрипты для вычислений и проверок, система CyberTrace.
- Поддерживаются только точки назначения типа **storage**, **correlator**, **internal**, у которых отсутствует дисковый буфер.
- Поле `S.KL_EventRoute` не добавляется к корреляционному событию.
- Коррелятор не может обогащать корреляционное событие дополнительными полями `SourceAssetKSCInstanceID`, `SourceAssetKSCHostID`, `DestinationAssetKSCInstanceID`, `DestinationAssetKSCHostID`, `DeviceAssetKSCInstanceID`, `DeviceAssetKSCHostIDKSC`, `S.KL_SourceAccountDisplayName`, `S.KL_DestinationAccountDisplayName`.
- Поддержка шаблонов неполная: некоторые шаблоны могут не обрабатываться, функции типа `to_string` работают не во всех случаях.
- Доступно ограниченное количество метрик.
- Параметр `debug` не изменяет уровень журналирования.
- Содержимое контейнеров можно экспортировать только в формате JSON. Импорт и поиск по содержимому контейнеров недоступны.
- Сбор и анализ статистики работы коррелятора для оптимизации производительности не поддерживается.
- Регулярные выражения не поддерживают конструкции типа `(?=...)` и `(?<=...)`.
- Ссылки на активные листы, контекстные таблицы, словари и категории активов должны задаваться через уникальные идентификаторы, а не через имена.

Настройка коррелятора correlator-ng

> В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

Коррелятор correlator-ng разворачивается как отдельный сервис KUMA. Его работа определяется конфигурационными файлами в формате YAML и параметрами запуска процесса. После старта сервис устанавливает соединение с Ядром KUMA, получает конфигурацию правил и контейнеров и переходит к обработке событий.

Коррелятор correlator-ng управляется через набор YAML-файлов. Ниже приводится описание каждого файла.

Конфигурационные файлы correlator-ng

Файл	Описание
config.yaml	Содержит базовую информацию о сервисе, включая имя коррелятора, описание и общие параметры работы.
correlation-rules.yaml	Содержит конфигурацию правил корреляции, включая типы правил: standard, simple, operational and periodical.
selector-includes.yaml	Содержит вложенные фильтры, которые привязываются к правилам корреляции для их повторного использования.
active-lists.yaml	Содержит конфигурацию активных листов.
context-tables.yaml	Содержит конфигурацию контекстных таблиц.
dictionaries.yaml	Содержит статические словари для использования в селекторах и правилах корреляции.
global-variables.yaml	Содержит глобальные переменные, доступные в правилах корреляции и селекторах.
destinations.yaml	Содержит точки назначения событий (`storage`, `correlator`, `internal`) с указанием идентификаторов и параметров отправки.

Файлы загружаются при запуске коррелятора в следующем порядке: сначала config.yaml, затем файлы с правилами и селекторами, затем файлы с активными листами, контекстными таблицами, словарями и глобальными переменными. Файл с точками назначения загружается последним, чтобы гарантировать правильную маршрутизацию событий.

Systemd-unit и запуск коррелятора

Для запуска коррелятора как системного сервиса используется unit-файл systemd, который определяет параметры запуска, остановки и перезапуска correlator-ng.

Пример файла:

```
[Unit]
Description=KUMA Correlator NG
StartLimitIntervalSec=1
After=network.target

[Service]
Type=simple
Restart=always
RestartPreventExitStatus=99
TimeoutSec=0
RestartSec=5

Environment="RUST_BACKTRACE=full"

User=kuma
Group=kuma

ExecStart=/opt/kuma correlator --id <идентификатор_сервиса_коррелятора> --core https://<FQDN_Ядра_KUMA>:7210 --wd
/opt/correlator-ng --api.port <API-порт_коррелятора>
LimitFSIZE=infinity
LimitCPU=infinity
LimitAS=infinity
LimitNOFILE=500000
LimitNPROC=64000
LimitMEMLOCK=infinity
TasksMax=infinity
TasksAccounting=false

[Install]
WantedBy=multi-user.target
```

Журналирование correlator-ng

Уровень журналирования correlator-ng задается параметром запуска `--logger.filter`. Параметр принимает те же значения уровней журналирования, что и стандартная переменная `RUST_LOG`: `trace`, `debug`, `info`, `warn`, `error`.

Пример:

```
--logger.filter debug
```

Дополнительно можно использовать переменную окружения `RUST_BACKTRACE`. При значении `full` включается расширенное отображение информации об ошибках.

Поддерживаемые типы данных correlator-ng

> В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

В корреляторе correlator-ng реализована более строгая модель данных по сравнению со стандартной версией коррелятора. Это влияет на правила корреляции, работу селекторов и функции обработки событий. Каждое поле события, переменной или селектора теперь имеет заранее определенный тип. Автоматическое приведение типов применяется только для совместимых типов, в остальных случаях используется приведение через функции `to_string`, `to_integer`, `to_float`.

Поддерживаются следующие типы данных

Поддерживаемые типы данных

Тип данных	Описание
Строка	Строка
VecString	Массив строк
I64	Целое число 64-бит
VecI64	Массив целых чисел 64-бит
F64	Число с плавающей точкой
VecF64	Массив чисел с плавающей точкой
Timestamp	Временная метка в формате UNIX Timestamp (в миллисекундах)
VecTimestamp	Массив временных меток в формате UNIX Timestamp (в миллисекундах)
Uuid	Уникальный идентификатор формата UUIDv4
VecUuid	Массив UUIDv4
Ip	IP-адрес формата IPv4 или IPv6
VecIp	Массив IP-адресов
IpNet	Подсеть с указанием префикса CIDR, например, `192.168.1.0/24`.
VecIpNet	Массив подсетей
Bool	Логическое значение `true` или `false`
VecBool	Массив логических значений

Более строгая типизация повышает эффективность работы коррелятора и уменьшает ошибки при компиляции правил корреляции. При этом все операции с массивами, строками и временными метками должны учитывать тип данных, иначе возможны ошибки выполнения.

Селекторы правил корреляции и выражения

В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

В correlator-ng селекторы обладают всеми возможностями переменных и могут использовать функции для работы со строками, массивами и числами (например, `substring`, `tr`, `to_lower`). Создавать отдельную переменную для использования функций не обязательно, селекторы сами могут применять эти функции.

Селекторы описываются с использованием SQL-синтаксиса, применимого для условий `WHERE`.

В конфигурации селекторов и переменных используются выражения для фильтрации и объединения событий. Они поддерживают те же операции, что и переменные, с возможностью построения сложных условий. Ниже приведены доступные типы выражений.

При написании выражений для сравнения значений с использованием констант следует указывать константу справа. В этом случае коррелятор применяет различные оптимизации. Если константа указана слева, то оптимизация не выполняется.

Константы

Константы

Константа	Тип
`1`	I64 (целое число)
`3.14`	F64 (число с плавающей точкой)
`'myString'`	String (строка)

Ссылки на значения

Ссылки на значения

Ссылка	Описание
`DeviceVendor`	Значение поля события `DeviceVendor`
`S.MyCustomField`	Значение композитного поля события `S.MyCustomField`
`$myVariable`	Значение переменной `myVariable`

Логические и групповые операторы

Логические и групповые операторы

Выражение	Описание
`<выражение> AND <выражение>`	Логический оператор И
`<выражение> OR <выражение>`	Логический оператор ИЛИ

Выражение	Описание
`NOT <выражение>`	Отрицание результата выражения
`IS [NOT] NULL`	Проверка на отсутствие значения (в correlator-ng отсутствующее значение обозначается `NULL`)
`()`	Группировка выражений

Сравнительные операторы

Сравнительные операторы

Выражение	Описание
`<выражение> = <выражение>`	Проверка на равенство значений
`<выражение> > <выражение>`	Сравнение значение с помощью оператора `>`
`<выражение> >= <выражение>`	Сравнение значение с помощью оператора `>=`
`<выражение> < <выражение>`	Сравнение значение с помощью оператора `<`
`<выражение> <= <выражение>`	Сравнение значение с помощью оператора `<=`
`Type BETWEEN 1 AND 3`	Проверка, находится ли значение поля `Type` между 1 и 3 включительно

Арифметические операторы

Арифметические операторы

Выражение	Описание
`<выражение> + <выражение>`	Сложение
`<выражение> - <выражение>`	Вычитание
`<выражение> * <выражение>`	Умножение
`<выражение> / <выражение>`	Деление
`<выражение> % <выражение>`	Деление по модулю

Функции

Функции

Функция	Описание
`eq_fold(<выражение левого операнда>, <выражение правого операнда>)`	Вызов функции `eq_fold`.

Подробнее о доступных функциях см. раздел Функции обработки данных в correlator-ng.

Атрибуты правила корреляции standard

> В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

Правило корреляции типа **standard** в correlator-ng поддерживает дополнительные атрибуты, которые позволяют изменить условия определения полного совпадения и задать сопоставление событий между селекторами. Эти атрибуты расширяют стандартную модель работы контейнера правила корреляции и применяются на этапе анализа событий, уже помещенных в контейнер.

В текущей реализации correlator-ng поддерживаются два атрибута:

- `anyMatch`
- `joinSelector`

Оба атрибута применимы только к правилам корреляции типа **standard** и используются непосредственно в конфигурации самого правила.

Атрибут anyMatch

В стандартной модели коррелятора правило корреляции считается выполненным, когда контейнер достигает состояния Полное совпадение, то есть все селекторы накопили количество событий, равное своим пороговым значениям.

Если в конфигурации правила корреляции указано `anyMatch: true`, контейнер считается достигшим состояния Полное совпадение, когда любой из селекторов правила (за исключением селекторов типа **recovery**) достигает своего порогового значения. Таким образом, правило срабатывает по первому выполненному условию, не ожидая накопления событий другими селекторами. Каждый селектор продолжает независимо накапливать события согласно своей конфигурации, однако завершение корреляции происходит сразу после достижения порога одним из них.

Корреляционное событие, сформированное таким правилом, дополнительно содержит локальную переменную `$KL_selectorName`. Значение переменной равно тегу селектора, достижение порога которого привело к срабатыванию правила. Это позволяет определить источник срабатывания и использовать различную дальнейшую обработку результата.

> Правило с атрибутом `anyMatch` не поддерживает триггер типа **По истечении времени жизни контейнера**.

Атрибут joinSelector

В стандартной модели коррелятора правило корреляции считается выполненным, когда контейнер достигает состояния Полное совпадение, то есть все селекторы накопили количество событий, равное своим пороговым значениям.

Если в конфигурации правила корреляции указано `anyMatch: true`, контейнер считается достигшим состояния Полное совпадение, когда любой из селекторов правила (за исключением селекторов типа **recovery**) достигает своего порогового значения. Таким образом, правило срабатывает по первому выполненному условию, не ожидая накопления событий другими селекторами. Каждый селектор продолжает независимо накапливать события согласно своей конфигурации, однако завершение корреляции происходит сразу после достижения порога одним из них.

Корреляционное событие, сформированное таким правилом, дополнительно содержит локальную переменную `$KL_selectorName`. Значение переменной равно тегу селектора, достижение порога которого привело к срабатыванию правила. Это позволяет определить источник срабатывания и использовать различную дальнейшую обработку результата.

> Правило с атрибутом `anyMatch` не поддерживает триггер типа **По истечении времени жизни контейнера**.

Атрибут joinSelector

Атрибут `joinSelector` позволяет дополнительно проверить взаимосвязь событий, накопленных разными селекторами внутри одного контейнера перед тем, как он достигнет состояние Полное совпадение.

Значением атрибута является SQL-подобное выражение: `joinSelector: < выражение >`

Выражение задает условие сравнения событий различных селекторов. Оно должно представлять собой бинарную операцию или функцию, операндами которой могут быть только константы и выражения вида `with_selector('< тег_селектора >', < выражение >)`.

Функция `with_selector` указывает, что выражение вычисляется относительно событий конкретного селектора.

При разборе конфигурации коррелятор автоматически определяет минимальное пороговое значение срабатывания селектора среди селекторов, участвующих в выражении. Сравнение выполняется только для количества событий, равного этому минимальному значению.

Например:

Порог срабатывания селектора (количество событий) селектора A равен 5, а у селектора B он равен 9. В выражении `with_selector('A', DeviceHostName) = with_selector('B', DeviceHostName)` будут сравниваться только первые пять событий каждого селектора.

События сопоставляются параллельно в порядке их поступления: первое событие селектора A сравнивается с первым событием селектора B; второе – со вторым, и так далее.

Атрибут `joinSelector` также может использовать функции. Например: `joinSelector: contains_fold(with_selector('A', $var_A), with_selector('B', DeviceCustomString1))`

В этом примере используется функция `contains_fold`, которая проверяет наличие значения переменной коррелятора `$var_A`, вычисленного для селектора A, в поле `DeviceCustomString1` событий селектора B без учета регистра.

В выражениях атрибута `joinSelector` не поддерживаются следующие функции:

- `has_ti_detect`
- `has_ti_detect_with_category`
- `has_ti_detect_with_indicator`
- `has_ti_detect_with_category_and_indicator`

Функции обработки данных в корреляторе-ng

> В текущей версии Kaspersky EDR Expert представлена бета-версия correlator-ng, которая предназначена для ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

В correlator-ng функции используются в селекторах и переменных для работы с данными событий, преобразования типов данных и фильтрации.

Общие правила синтаксиса:

- Обязательные аргументы заключаются в `< >`, опциональные – в `[ ]`.
- Неопределенное число аргументов обозначается `...`.
- Тип возвращаемого значения указывается как `-> <тип данных>`. Если указано `T`, тип зависит от типа аргументов.
- Тип аргументов может быть конкретным (например, `String`, `I64`.) или `T`, означающим любой доступный тип данных.

Функции для приведения типа данных

Используются для приведения значений к нужному типу данных.

Функции для приведения типа данных

Функция	Описание
`to_string(< выражение >)`	Преобразует значение в строку.
`to_integer(< выражение >)`	Преобразует значение в целое число (I64).
`to_float(< выражение >)`	Преобразует значение в число с плавающей точкой (F64).
`to_uuid(< выражение >)`	Преобразует значение в UUIDv4.
`to_ip(< выражение >)`	Преобразует значение в IP (v4 или v6).
`to_ip_net(< выражение >)`	Преобразует значение в подсеть IPNet.
`to_bool(< выражение >)`	Преобразует значение в логический тип.
`to_timestamp(< выражение >, '[ часовой_пояс ]')`	Преобразует значение во временную метку с возможностью указания часового пояса.

Функции для сравнения значений

Функции для сравнения значений

Функция	Описание
`eq_fold(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет, совпадает ли левое значение с правым без учета регистра.
`eq_any(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет, совпадает ли одно из правых значений с левым.
`eq_any_fold(< левый_операнд >, < правый_операнд >, [...]) -> Bool`	Сравнивает левое значение с множеством правых без учета регистра.
`contains(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет вхождение правого значения в левое.
`contains_fold(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет вхождение правого значения в левое без учета регистра.
`contains_any(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет вхождение любого из правых значений в левое.
`contains_any_fold(< левый_операнд >, < правый_операнд >, [...]) -> Bool`	Проверяет вхождение любого из правых значений в левое без учета регистра.
`starts_with(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет, является ли правое значение префиксом левого.
`starts_with_fold(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет префикс без учета регистра.
`starts_with_any(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет, является ли одно из правых значений префиксом левого.

Функция	Описание
`starts_with_any_fold(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет префикс без учета регистра для одного из правых значений.
`ends_with(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет, является ли правое значение суффиксом левого.
`ends_with_fold(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет суффикс без учета регистра.
`ends_with_any(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет, является ли одно из правых значений суффиксом левого.
`ends_with_any_fold(< левый_операнд >, < правый_операнд 1>, [...]) -> Bool`	Проверяет суффикс без учета регистра.
`match(< левый_операнд >, < правый_операнд >) -> Bool`	Проверяет, совпадает ли левое значение с регулярным выражением справа.
`match_any(< левый_операнд >, '< правый_операнд 1>', '[ правый_операнд 2]', [...]) -> Bool`	Проверяет, совпадает ли левое значение с одним из регулярных выражений справа.

Функции для работы с активными листами, словарями и контекстными таблицами

Функции для работы с активными листами, словарями и контекстными таблицами

Функция	Описание
`in_active_list('< идентификатор_активного_листа >', < элемент_ключа 1>, [...]) -> Bool`	Проверяет наличие значения в активном листе по ключу.
`in_context_table('< идентификатор_контекстной_таблицы >', '< имя_ключевого_поля 1>', < значение_ключевого_поля 1>, '[ имя_ключевого_поля 2]', [ значение_ключевого_поля 2], [...]) -> Bool`	Проверяет наличие значения в контекстной таблице по ключу.
`in_dictionary('< идентификатор_ словаря >', < элемент_ключа 1>, [ элемент_ключа 2], ...) -> Bool`	Проверяет наличие значения в словаре по ключу.
`dict('< идентификатор_словаря >', < ключ 1>, [...]) -> String`	Возвращает значение из словаря по ключу.
`table_dict('< идентификатор_словаря >', < имя_столбца >, < ключ 1>, [...]) -> String`	Возвращает значение из словаря-таблицы.
`active_list('< идентификатор_активного_листа >', < имя_поля >, < ключ 1>, [...]) -> String`	Возвращает значение из активного листа.
`context_table('< идентификатор_контекстной_таблицы >', '< имя_поля >', '< ключевое_поле >', < значение >) -> T`	Возвращает значение поля из контекстной таблицы.
`context_table_list_item('< идентификатор_контекстной_таблицы >', '< имя_поля >', < индекс >, ...) -> T`	Возвращает элемент массива из контекстной таблицы.
`match_active_list(...)`	Возвращает значение из активного листа, если ключ совпадает с регулярным выражением.
`match_context_table(...)`	Возвращает значение из контекстной таблицы при совпадении с регулярным выражением.
`match_dictionary(...)`	Возвращает значение из словаря при совпадении с регулярным выражением.

Функции работы с подсетями

Функции работы с подсетями

Функция	Описание
`in_subnet(< левый_операнд >, < подсеть >) -> Bool`	Проверяет принадлежность IP-адреса подсети.
`in_subnet_any(< левый_операнд >, < подсеть 1>, [...]) -> Bool`	Проверяет принадлежность IP-адреса одной из подсетей.
`in_subnet_active_list(...)`	Проверяет принадлежность IP-адреса подсети из активного листа.
`in_subnet_context_table(...)`	Проверяет принадлежность IP-адреса подсети из контекстной таблицы.
`in_subnet_dictionary(...)`	Проверяет принадлежность IP-адреса подсети из словаря.

Функции обработки строк

Функции обработки строк

Функция	Описание
`to_lower(< операнд >) -> String`	Приводит строку к нижнему регистру.
`to_upper(< операнд >) -> String`	Приводит строку к верхнему регистру.
`substring(< строка >, < начало_подстроки >, [ конец_подстроки ]) -> String`	Возвращает подстроку.
`index_of(< что_искать >, < где_искать >) -> I64`	Возвращает позицию первого вхождения.
`last_index_of(< что_искать >, < где_искать >) -> I64`	Возвращает позицию последнего вхождения.
`tr(< операнд >) -> String`	Удаляет пробельные символы в начале и конце строки.
`replace(< строка >, < подстрока >, < замена >) -> String`	Заменяет подстроку.
`regexp_replace(< строка >, '< регулярное_выражение >', '< замена >') -> String`	Выполняет замену с использованием регулярного выражения.
`regexp_capture(< строка >, '< регулярное_выражение >') -> String`	Извлекает подстроку по регулярному выражению.
`str_join('< разделитель >', < строка 1>, [...]) -> String`	Объединяет несколько строк.

Функции работы с массивами

Функции работы с массивами

Функция	Описание
`append(< левый операнд >, < правый операнд >, '[ разделитель ]') -> T`	Добавляет значение в конец массива или строки.
`prepend(< левый операнд >, < правый операнд >, '[ разделитель ]') -> T`	Добавляет значение в начало массива или строки.
`len(< операнд >) -> I64`	Возвращает длину строки или массива.
`item(< массив >, < индекс >) -> T`	Возвращает элемент массива по индексу.
`distinct_items(< массив >) -> T`	Удаляет дубликаты элементов массива.
`sort_items(< массив >, '< порядок_сортировки >') -> T`	Сортирует элементы в массиве.

Функции работы с временными метками

Функции работы с временными метками

Функция	Описание
`now() -> Timestamp`	Возвращает текущую временную метку.
`year(<timestamp>) -> I64`	Возвращает год.
`month(<timestamp>) -> I64`	Возвращает номер месяца.
`month_str(<timestamp>) -> String`	Возвращает месяц в строковом виде.
`weekday(<timestamp>) -> I64`	Возвращает номер дня недели.
`weekday_str(<timestamp>) -> String`	Возвращает день недели в строковом виде.
`day(<timestamp>) -> I64`	Возвращает день месяца.
`hour(<метка_времени>) -> I64`	Возвращает час.
`minute(<timestamp>) -> I64`	Возвращает минуту.
`second(<timestamp>) -> I64`	Возвращает секунду.
`millisecond(<timestamp>) -> I64`	Возвращает миллисекунду.
`format_timestamp(<timestamp>, '< формат >') -> String`	Преобразует временную метку в строку.
`truncate_timestamp(<timestamp>, '< длительность >') -> Timestamp`	Округляет временную метку до целого значения.

Функции вычисления времени

Функции вычисления времени

Функция	Описание
`duration_days(<t1>, <t2>) -> I64`	Возвращает разницу в днях.
`duration_hours(<t1>, <t2>) -> I64`	Возвращает разницу в часах.
`duration_minutes(<t1>, <t2>) -> I64`	Возвращает разницу в минутах.
`duration_seconds(<t1>, <t2>) -> I64`	Возвращает разницу в секундах.
`duration_milliseconds(<t1>, <t2>) -> I64`	Возвращает разницу в миллисекундах.

Математические функции

Математические функции

Функция	Описание
`round(< операнд >) -> I64`	Округляет значение до ближайшего целого.
`ceil(< операнд >) -> I64`	Округляет значение вверх.
`floor(< операнд >) -> I64`	Округляет значение вниз.
`abs(< операнд >) -> T`	Возвращает модуль числа.
`pow(< операнд >, '< степень >') -> T`	Возводит число в степень.
`math_min(< массив >) -> T`	Возвращает минимальный элемент массива.
`math_max(< массив >) -> T`	Возвращает максимальный элемент массива.
`math_avg(< массив >) -> F64`	Вычисляет среднее значение массива.

Функции декодирования и анализа данных

Функции декодирования и анализа данных

Функция	Описание
`decode_hex_integer(< строка >) -> I64`	Преобразует hex-строку в число.
`decode_hex(< строка >) -> String`	Декодирует hex-строку.
`decode_base64(< строка >) -> String`	Декодирует строку Base64.
`decode_url(< строка >) -> String`	Декодирует URL-кодированную строку.
`entropy(< строка >) -> F64`	Вычисляет энтропию Шеннона строки.
`has_bit(< левый операнд >, < позиция >) -> Bool`	Проверяет, установлен ли бит в указанной позиции.
`has_vulnerability(< идентификатор_актива >, (<CVE>), [ критичность ]) -> Bool`	Проверяет наличие уязвимости у актива.

Другие функции

Другие функции

Функция	Описание
`include('< идентификатор_предиката >', '[ имя_предиката ]')`	Использует заранее определенные предикаты из файла selector-includes.yaml.
`ti('< категория >', < индикатор >, '< поле >')`	Извлекает значение из специализированного поля TI (CyberTrace).
`with_selector(' тег_селектора_правила_корреляции ', < выражение >)`	Может использоваться только в атрибуте `joinSelector` правила корреляции для различения наборов событий.
`template('< шаблон >', [ аргумент 1], [ аргумент 2], ...) -> String`	Формирует строку на основе шаблона, подставляя в него значения полей события или переменных.
`conditional('< предикат >', <then>, <else>)`	Возвращает одно из двух значений, в зависимости от результата предиката
`has_ti_detect*()`	Проверяет наличие срабатывания CyberTrace по категории или индикатору.
`has_ti_detect_with_category('< категория >')`	Проверяет наличие срабатывания CyberTrace по категории.
`has_ti_detect_with_indicator(< индикатор >)`	Проверяет наличие срабатывания CyberTrace по индикатору.
`has_ti_detect_with_category_and_indicator('< категория >', < индикатор >)`	Проверяет наличие срабатывания CyberTrace по категории и индикатору.

Настройка источников событий

В этом разделе представлена информация о настройке получения событий из разных источников.

Настройка получения событий Auditd

KUMA позволяет осуществлять мониторинг и проводить аудит событий Auditd на устройствах Linux.

Перед настройкой получения событий убедитесь, что вы создали коллектор KUMA для событий Auditd.

Настройка получения событий Auditd состоит из следующих этапов:

1. Установка коллектора KUMA в сетевой инфраструктуре.
2. Настройка сервера источника событий.
3. Проверка поступления событий Auditd в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно, выполнив поиск связанных событий в Консоли KUMA.

Установка коллектора KUMA для получения событий Auditd

После создания коллектора для настройки получения событий с помощью rsyslog требуется установить коллектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка сервера источника событий

Для передачи событий от сервера в коллектор KUMA используется служба rsyslog.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере источнике событий установлена служба rsyslog. Для этого выполните команду:

   ```
   systemctl status rsyslog.service
   ```

   Если служба rsyslog не установлена на сервере, установите ее, выполнив следующую команду:

   - для дистрибутивов на базе RPM:

     ```
     yum install rsyslog
     ```

   - для дистрибутивов на базе Debian или Ubuntu:

     ```
     apt-get install rsyslog
     ```

   Включите службу, выполнив команду:

   ```
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В папке /etc/rsyslog.d создайте файл audit.conf со следующим содержанием:

   ```
   $ModLoad imfile
   $InputFileName /var/log/audit/audit.log
   $InputFileTag tag_audit_log:
   $InputFileStateFile audit_log
   $InputFileSeverity info
   $InputFileFacility local6
   $InputRunFileMonitor
   *.* @<ip адрес коллектора KUMA>:<порт коллектора KUMA>
   ```

Если вы хотите отправлять события по протоколу TCP, вместо последней строки в файле вставьте следующую:
```
*.* @@<ip адрес коллектора KUMA>:<порт коллектора KUMA>.
```

3. Сохраните изменения в файле audit.conf.

4. Перезапустите службу rsyslog, выполнив следующую команду:
```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор KUMA.

Настройка получения событий KATA/EDR

Вы можете настроить получение событий приложения Kaspersky Anti Targeted Attack Platform в SIEM-систему KUMA.

Перед настройкой получения событий убедитесь, что вы создали коллектор KUMA для событий KATA/EDR.

При создании коллектора в Консоли KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c Настройка для передачи событий Kaspersky Anti Targeted Attack Platform в KUMA, а тип коннектора соответствует типу, указанному в пункте 4d.

Для получения событий Kaspersky Anti Targeted Attack Platform с помощью syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Настройка получения событий KATA/EDR состоит из следующих этапов:

1. Настройка пересылки событий KATA/EDR

2. Установка коллектора KUMA в сетевой инфраструктуре

3. Проверка поступления событий KATA/EDR в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KATA/EDR выполнена правильно, выполнив поиск связанных событий в Консоли KUMA. События Kaspersky Anti Targeted Attack Platform отображаются в таблице с результатами поиска как KATA.

Настройка передачи событий KATA/EDR в KUMA

Чтобы настроить передачу событий из приложения Kaspersky Anti Targeted Attack Platform в KUMA:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. В окне ввода учетных данных пользователя установите флажок **Локальный администратор** и введите данные Администратора.

3. Перейдите в раздел **Параметры** → **SIEM-система**.

4. Задайте следующие параметры:

   a. Установите флажки **Журнал активности** и **Обнаружения**.

   b. В поле **Устройство/IP** введите IP-адрес или имя устройства коллектора KUMA.

   c. В поле **Порт** укажите номер порта подключения к коллектору KUMA.

   d. В поле **Протокол** выберите из списка **TCP** или **UDP**.

   e. В поле **ID устройства** укажите идентификатор устройства сервера, который будет указан в журнале SIEM-систем как источник обнаружения.

   f. В поле **Периодичность сигнала** введите интервал отправки сообщений: от 1 до 59 минут.

   g. При необходимости, включите TLS-шифрование.

   h. Нажмите **Применить**.

Передача событий Kaspersky Anti Targeted Attack Platform в KUMA настроена.

Создание коллектора KUMA для получения событий KATA/EDR

После того как параметры передачи событий настроены, требуется создать коллектор в Консоли KUMA для событий Kaspersky Anti Targeted Attack Platform.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

> При создании коллектора в Консоли KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c Настройка для передачи событий Kaspersky Anti Targeted Attack Platform в KUMA, а тип коннектора соответствует типу, указанному в пункте 4d.

> Для получения событий Kaspersky Anti Targeted Attack Platform с помощью syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Установка коллектора KUMA для получения событий KATA/EDR

После создания коллектора для настройки получения событий Kaspersky Anti Targeted Attack Platform требуется установить новый коллектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Интеграция с другими решениями

В этом разделе описано, как интегрировать KUMA с другими приложениями для расширения возможностей приложения.

Интеграция с Kaspersky Security Center

Вы можете создавать или изменять параметры интеграции Kaspersky Security Center в Консоли OSMP.

В Консоли OSMP вы можете просмотреть интеграцию с выбранными Серверами администрирования Kaspersky Security Center для одного, нескольких или всех тенантов KUMA. Если включена интеграция с Kaspersky Security Center, вы можете выполнить импорт активов вручную, отредактировать интервал автоматического импорта по расписанию или временно выключить импорт по расписанию.

Настройка интервала обновления данных для активов Kaspersky Security Center

KUMA импортирует следующие данные об устройстве, полученные от Агентов администрирования Kaspersky Security Center:

- основную информацию об активе – имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании, состоянии защиты, версии антивирусных баз;
- информацию об атрибутах актива – об уязвимостях, о программном обеспечении, включая операционную систему, о владельцах.

Чтобы настроить интервал обновления данных об активе из Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, в который вы хотите импортировать данные активов KSC.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Параметры активов**.
4. Убедитесь, что на вкладке **Импорт KSC** включен переключатель **Состояние**.

5. Укажите интервалы для автоматического импорта информации об активах и уязвимостях активов из Kaspersky Security Center, выполнив следующие действия:

   - В разделе **Информация об оборудовании** в поле **Интервал импорта (в часах)** введите интервал в часах, в котором информация о базовых атрибутах активов будет импортироваться автоматически. Значение по умолчанию – 1 час.

   - В разделе **Атрибуты активов** в поле **Интервал импорта (в часах)** введите интервал в часах, в котором информация о других атрибутах активов будет импортироваться автоматически. Значение по умолчанию: 12 часов.

     Поскольку во время импорта информации об атрибутах активов (уязвимостях, программном обеспечении, владельцах) может загружаться большое количество данных и для его выполнения требуется более длительное время, рекомендуется задавать для него больший интервал, чем для импорта информации об оборудовании.

6. Нажмите на кнопку **Сохранить**.

Параметры обновления данных активов Kaspersky Security Center для выбранного тенанта настроены.

Если нужный тенант отсутствует в списке тенантов, используйте OSMP Console, чтобы добавить его в список тенантов.

Расписание импорта активов Kaspersky Security Center

Чтобы настроить расписание импорта активов Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Выберите тенант, для которого вы хотите запланировать импорт активов Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

4. При необходимости снимите флажок **Выключено**, чтобы включить интеграцию с Kaspersky Security Center для выбранного тенанта. По умолчанию флажок снят.

   Если вы хотите временно выключить интеграцию с Kaspersky Security Center для выбранного тенанта, установите флажок **Выключено**. Импорт активов Kaspersky Security Center по расписанию выключен.

5. В поле **Период обновления данных** укажите период времени, по истечении которого KUMA обновляет данные об устройствах Kaspersky Security Center.

   Интервал указывается в часах и должен быть целым числом.

   По умолчанию временной интервал составляет 12 часов.

6. Нажмите на кнопку **Сохранить**.

Указанные параметры для импорта активов Kaspersky Security Center по расписанию для выбранного тенанта применены.

Ручной импорт активов Kaspersky Security Center

KUMA импортирует следующие данные об устройстве, полученные от Агентов администрирования Kaspersky Security Center:

- основную информацию об активе – имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании, состоянии защиты, версии антивирусных баз;
- информацию об атрибутах актива – об уязвимостях, о программном обеспечении, включая операционную систему, о владельцах.

Чтобы вручную импортировать активы Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, в который вы хотите импортировать данные активов KSC.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Параметры активов**.
4. Убедитесь, что на вкладке **Импорт KSC** включен переключатель **Состояние**.
5. Укажите интервалы для автоматического импорта информации об активах и уязвимостях активов из Kaspersky Security Center, выполнив следующие действия:
   - Чтобы импортировать информацию об основных атрибутах активов, в разделе **Информация об оборудовании** нажмите на кнопку **Импорт**.
   - Чтобы импортировать информацию о других атрибутах активов, в разделе **Атрибуты активов** нажмите на кнопку **Импорт**.

Будет создана задача по *импорту активов KSC*. Активы Kaspersky Security Center для указанного тенанта импортируются независимо от настроенного расписания.

Просмотр иерархии Серверов администрирования Kaspersky Security Center

Чтобы просмотреть иерархию Серверов администрирования Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.
2. В разделе **Интеграции** нажмите **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.
3. В раскрывающемся списке **Тенант** выберите тенант, для которого вы хотите просмотреть иерархию.

   Откроется окно **Параметры подключения**.
4. В окне **Параметры подключения** нажмите **Загрузить иерархию**.

Иерархия Серверов администрирования Kaspersky Security Center для указанного тенанта отображается в окне **Параметры подключения**.

Импорт событий из базы Kaspersky Security Center

В KUMA можно получать события из SQL-базы Kaspersky Security Center. Получение событий производится с помощью коллектора, в котором используются следующие ресурсы:

- Предустановленный коннектор [OOTB] KSC MSSQL или [OOTB] KSC MySQL.
- Предустановленный нормализатор [OOTB] KSC from SQL.

Настройка импорта событий из Kaspersky Security Center состоит из следующих шагов:

1. Создание копии предустановленного коннектора.

   Параметры предустановленного коннектора недоступны для редактирования, поэтому для настройки параметров подключения к серверу базы данных требуется создать копию предустановленного коннектора.

2. Создание коллектора:

   - В веб-интерфейсе.
   - На сервере.

Чтобы настроить импорт событий из Kaspersky Security Center:

1. Создайте копию предустановленного коннектора, соответствующего типу базы данных Kaspersky Security Center:

   a. В Консоли OSMP в разделе **Мониторинг** → **Ресурсы** → **Коннекторы** найдите в структуре папок нужный предустановленный коннектор, установите флажок рядом с этим коннектором и нажмите **Дублировать**.

   b. В открывшемся окне **Создание коннектора** на вкладке **Основные параметры** в поле **Запрос по умолчанию** при необходимости замените имя базы данных KAV на имя используемой вами базы данных Kaspersky Security Center.

   Пример запроса к SQL-базе Kaspersky Security Center

   ```
   SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

       ev.product_name AS product_name, ev.product_version AS product_version,

        ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As msg,

   CASE

       WHEN ev.rise_time is not NULL THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time )

          ELSE ev.rise_time

       END
   ```

```
AS endTime,
CASE
   WHEN ev.registration_time is not NULL
      THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )
      ELSE ev.registration_time
   END
AS kscRegistrationTime,
cast(ev.par7 as varchar(4000)) as sourceUserName,
hs.wstrWinName as dHost,
hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,
   CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +
CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +
CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +
CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,
serv.wstrWinDomain as kscNtDomain,
   CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +
CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +
CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +
CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,
CASE
WHEN virus.tmVirusFoundTime is not NULL
      THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )
      ELSE ev.registration_time
   END
AS virusTime,
virus.wstrObject As filePath,
virus.wstrVirusName as virusName,
virus.result_ev as result
```

FROM KAV.dbo.ev_event as ev

LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId

INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1

Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus

where registration_time >= DATEADD(minute, -191, GetDate())

c. Установите курсор в поле **URL** и в раскрывшемся списке в строке используемого секрета нажмите на значок ✎.

d. В открывшемся окне **Секрет** в поле **URL** укажите адрес для подключения к серверу в следующем формате:

```
sqlserver://user:password@kscdb.example.com:1433/database
```

где:

- `user` – учетная запись с правами public и db_datareader к нужной базе данных;
- `password` – пароль учетной записи;
- `kscdb.example.com:1433` – адрес и порт сервера базы данных;
- `database` – название базы данных Kaspersky Security Center. По умолчанию – KAV.

Нажмите на кнопку **Сохранить**.

e. В окне **Создание коннектора** в разделе **Подключение** в поле **Запрос** при необходимости замените имя базы данных KAV на имя используемой вами базы данных Kaspersky Security Center.

Это действие нужно выполнять, если вы планируете использовать столбец идентификатора, к которому относится запрос.

Нажмите на кнопку **Сохранить**.

2. Установите коллектор в веб-интерфейсе:

a. Запустите мастер установки коллектора одним из следующих способов:

- В Консоли OSMP в разделе **Мониторинг** → **Ресурсы** нажмите на кнопку **Подключить источник**.
- В Консоли OSMP в разделе **Мониторинг** → **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

b. На шаге 1 **Экспортировать источники событий** в мастере установки укажите название коллектора и выберите тенант.

c. На шаге 2 **Транспорт** в мастере установки выберите созданную на шаге 1 копию коннектора.

d. На шаге 3 **Парсинг событий** в мастере установки на вкладке **Схемы парсинга** нажмите **Добавить парсинг событий**.

e. В открывшемся окне **Основной парсинг событий** на вкладке **Схема нормализации** в раскрывающемся списке **Нормализатор** выберите **[OOTB] KSC from SQL** и нажмите **OK**.

f. При необходимости укажите остальные параметры в соответствии с вашими требованиями к коллектору. Для импорта событий настройка параметров на остальных шагах мастера установки не обязательна.

g. На шаге 8 **Проверка параметров** в мастере установки нажмите **Создать и сохранить сервис**.

В нижней части окна отобразится команда, которая понадобится для установки коллектора на сервере. Скопируйте эту команду.

h. Закройте мастер установки коллектора, нажав **Сохранить коллектор**.

3. Установите коллектор на сервере.

Для этого на сервере, предназначенном для получения событий Kaspersky Security Center, выполните команду, скопированную после создания коллектора в веб-интерфейсе.

В результате коллектор будет установлен и сможет принимать события из SQL-базы Kaspersky Security Center.

Вы можете просмотреть события Kaspersky Security Center в разделе веб-интерфейса **События**.

Интеграция с Kaspersky CyberTrace

Kaspersky CyberTrace (далее CyberTrace) – это инструмент, который объединяет потоки данных об угрозах с решениями SIEM. Он обеспечивает пользователям мгновенный доступ к данным аналитики, повышая их осведомленность при принятии решений, связанных с безопасностью.

Вы можете интегрировать CyberTrace с KUMA одним из следующих способов:

- Интегрировать функцию поиска индикаторов CyberTrace для обогащения событий KUMA информацией потоков данных CyberTrace.
- Интегрировать в KUMA веб-интерфейс CyberTrace целиком, чтобы обеспечить полный доступ к CyberTrace.

> Интеграция с консолью CyberTrace доступна только в том случае, если ваша лицензия CyberTrace включает многопользовательскую функцию.

Интеграция поиска по индикаторам CyberTrace

Чтобы выполнить интеграцию поиска по индикаторам CyberTrace, следует выполнить следующие шаги:

1. Настроить CyberTrace для приема и обработки запросов от KUMA.

Вы можете настроить интеграцию с KUMA сразу после установки CyberTrace в мастере первоначальной настройки или позднее в веб-интерфейсе CyberTrace.

2. Создать правила обогащения событий.

В правиле обогащения вы можете указать, какими данными из CyberTrace вы хотите дополнить событие.

3. Создать коллектор для получения событий, которые вы хотите обогатить данными из CyberTrace.

4. Привязать правило обогащения к коллектору.

5. Сохранить и создать службу:

   - Если вы привязали правило к новому коллектору, нажмите **Сохранить и создать**, в открывшемся окне скопируйте идентификатор коллектора и используйте скопированный идентификатор для установки коллектора на сервере через интерфейс командной строки.

   - Если вы привязали правило к уже существующему коллектору, нажмите **Сохранить и перезапустить службу**, чтобы применить параметры.

   Настройка интеграции поиска по индикаторам CyberTrace завершена и события KUMA будут обогащаться данными из CyberTrace.

Пример проверки обогащения данными из CyberTrace

По умолчанию проверка соединения с CyberTrace в KUMA отсутствует.

Если вы хотите проверить интеграцию с CyberTrace и убедиться, что обогащение событий выполняется, вы можете повторить шаги из следующего примера или адаптировать пример с учетом своих потребностей. В примере показана проверка интеграции, в результате которой обогащение будет выполнено и событие будет содержать заданный тестовый URL.

Чтобы выполнить проверку:

1. Создайте тестовое правило обогащения с параметрами, перечисленными в таблице ниже.

Параметр	Значение
Имя	Test CT enrichment
Тенант	Общий
Тип источника	CyberTrace
URL	<URL сервера cybertrace, которому вы хотите отправлять запросы>:9999
Сопоставление	Поле KUMA: RequestURL Индикатор CyberTrace: url
Отладка	Включено

1. Создайте тестовый коллектор со следующими параметрами:

   На шаге **2 Транспорт** укажите коннектор http.

   На шаге **3 Парсинг** событий укажите нормализатор и выберите метод парсинга json, задайте сопоставление полей RequestUrl – RequestUrl.

   На шаге **6 Обогащение** укажите правило обогащения Test CT enrichment.

   На шаге **7 Маршрутизация** укажите хранилище, куда следует отправлять события.

2. Нажмите на кнопку **Создать и сохранить службу**.

   В окне появится готовая команда для установки коллектора.

3. Нажмите **Копировать**, чтобы скопировать команду в буфер обмена, и запустите команду через интерфейс командной сроки. Дождитесь выполнения команды, вернитесь в Консоль KUMA и нажмите на кнопку **Сохранить коллектор**.

   Тестовый коллектор создан, и тестовое правило обогащения привязано к коллектору.

4. Через интерфейс командной строки отправьте в коллектор запрос, который вызовет появление события и последующее обогащение значением тестового URL `http://fakess123bn.nu`. Например:

```
curl --request POST \
  --url http://<идентификатор хоста, на котором установлен коллектор>:<порт коллектора>/input \
  --header 'Content-Type: application/json' \
  --data '{"RequestUrl":"http://fakess123bn.nu"}'
```

5. Перейдите в раздел KUMA **События** и выполните следующий запрос, чтобы ограничить выдачу событий и найти обогащенное событие:

```
SELECT * FROM `events` WHERE RequestUrl = 'http://fakess123bn.nu' ORDER BY Timestamp DESC LIMIT 250
```

Результаты:

Обогащение выполнено успешно, в событии появилось поле **RequestURL** со значением `http://fakess123bn.nu`, а также TI-индикатор и категория индикатора с данными CyberTrace.

Если в результате проверки обогащение не выполнено, например TI-индикатор отсутствует, рекомендуется:

1. Проверить параметры коллектора и правила обогащения.

2. Выгрузить журналы коллектора с помощью следующей команды и просмотреть полученные журналы на наличие ошибок:

```
tail -f /opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector
```

Настройка CyberTrace для приема и обработки запросов

Вы можете настроить CyberTrace для приема и обработки запросов от KUMA сразу после установки в мастере первоначальной настройки или позднее в веб-интерфейсе приложения.

Чтобы настроить CyberTrace для приема и обработки запросов в мастере первоначальной настройки:

1. Дождитесь запуска мастера первоначальной настройки CyberTrace после установки приложения.

   Откроется окно **Welcome to Kaspersky CyberTrace**.

2. В раскрывающемся списке **Выберите SIEM** выберите тип SIEM-системы, от которой вы хотите получать данные, и нажмите на кнопку **Далее**.

   Откроется окно **Параметры подключения**.

3. Выполните следующие действия:

   a. В блоке параметров **Service listens on** выберите вариант **IP and port**.

   b. В поле **IP address** введите `0.0.0.0`.

   c. В поле **Port** введите укажите порт для получения событий, порт по умолчанию `9999`.

   d. В блоке параметров **Service sends events to** в поле **IP address or hostname** укажите `127.0.0.1` и в поле **Port** укажите `9998`.

   Остальные значения оставьте по умолчанию.

   e. Нажмите на кнопку **Далее**.

Откроется окно **Параметры прокси-сервера**.

4. Если в вашей организации используется прокси-сервер, укажите параметры соединения с ним. Если нет, оставьте все поля незаполненными и нажмите на кнопку **Next**.

   Откроется окно **Licensing Settings**.

5. В поле **Kaspersky CyberTrace license key** добавьте лицензионный ключ для приложения CyberTrace.

6. В поле **Kaspersky Threat Data Feeds certificate** добавьте сертификат, позволяющий скачивать с серверов обновлений списки данных (data feeds), и нажмите на кнопку **Next**.

CyberTrace будет настроен.

Чтобы настроить CyberTrace для приема и обработки запросов в веб-интерфейсе приложения:

1. В веб-интерфейсе CyberTrace выберите раздел **Settings** – **Service**.

2. В блоке параметров **Connection Settings** выполните следующие действия:

   a. Выберите вариант **IP and port**.

   b. В поле **IP address** введите `0.0.0.0`.

   c. В поле **Port** укажите порт для приема событий, порт по умолчанию `9999`.

3. В блоке параметров **Web interface** в поле **IP address or hostname** введите `127.0.0.1`.

4. В верхней панели инструментов нажмите на кнопку **Restart the CyberTrace Service**.

5. Выберите раздел **Settings** – **Events format**.

6. В поле **Alert events format** введите `%Date% alert=%Alert%%RecordContext%`.

7. В поле **Detection events format** введите `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.

8. В поле **Records context format** введите `|%ParamName%=%ParamValue%`.

9. В поле **Actionable fields context format** введите `%ParamName%:%ParamValue%`.

CyberTrace будет настроен.

После обновления конфигурации CyberTrace требуется перезапустить сервер CyberTrace.

Создание правил обогащения событий

Чтобы создать правила обогащения событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила обогащения**.

2. В левой части окна выберите или создайте директорию, в которой будет храниться новое правило.

   Отобразится список доступных правил обогащения.

3. Нажмите **Создать**, чтобы создать новое правило.

   Откроется окно правила обогащения.

4. Укажите параметры правила обогащения:

   a. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип источника** выберите **cybertrace**.

   d. Укажите **URL** сервера CyberTrace, к которому вы хотите подключиться. Например, *example.domain.com:9999*.

   e. При необходимости укажите в поле **Количество подключений** максимальное количество подключений к серверу CyberTrace, которые может одновременно установить OSMP. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

   f. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять OSMP в секунду. По умолчанию указано значение `1000`.

   g. В поле **Максимальное количество событий в очереди обогащения** укажите максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1000000`.

   h. В поле **Время ожидания** укажите время в секундах, в течение которого OSMP должна ожидать ответа от сервера CyberTrace. Событие не будет отправлено в коррелятор, пока не истечет время ожидания или не будет получен ответ. Если ответ получен до истечения времени ожидания, он добавляется в поле события `TI`, и обработка события продолжается. По умолчанию указано значение `30`.

   i. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

   j. В раскрывающемся списке **Теги** выберите теги для правила обогащения событий.

   k. При необходимости в поле **Описание** добавьте до 4000 символов Юникода.

l. В блоке параметров **Сопоставление** требуется указать поля событий, которые следует отправить в CyberTrace на проверку, а также задать правила сопоставления полей событий KUMA с типами индикаторов CyberTrace:

- В столбце **Поле KUMA** выберите поле, значение которого требуется отправить в CyberTrace.
- В столбце **Индикатор CyberTrace** выберите тип индикатора CyberTrace для каждого выбранного поля:
  - **ip**
  - **url**
  - **hash**

В таблице требуется указать как минимум одну строку. Нажав на кнопку **Добавить**, можно добавить строку, а на кнопку ✕ – удалить.

m. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке **Фильтр** можно выбрать существующий фильтр или **Создать** новый фильтр.

Создание фильтра в ресурсах

Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.
2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.
3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.
4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:
   a. Нажмите на кнопку **Добавить условие**.
   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.
   c. В раскрывающемся списке **Оператор** выберите оператор.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку .

5. Нажмите на кнопку **Создать**.

Создано правило обогащения.

Интеграция поиска по индикаторам CyberTrace настроена. Созданное правило обогащения можно добавить к коллектору. Требуется перезапустить коллекторы KUMA, чтобы применить новые параметры.

Если какие-либо из полей CyberTrace в области деталей события содержат " [{ " или " }] ", это означает, что информация из потока данных об угрозах из CyberTrace была обработана некорректно и некоторые данные, возможно, не отображаются. Информацию из потока данных об угрозах можно получить, скопировав из события KUMA значение поля **TI indicator** событий и выполнив поиск по этому значению на портале CyberTrace в разделе индикаторов. Вся информация будет отображаться в разделе CyberTrace **Indicator context**.

Интеграция интерфейса CyberTrace

Вы можете интегрировать веб-интерфейс CyberTrace в Консоль OSMP. Когда эта интеграция включена, в Консоли OSMP появляется раздел **CyberTrace** с доступом к веб-интерфейсу CyberTrace. Вы можете настроить интеграцию в разделе **Настройки** → **KUMA** → **Открыть параметры KUMA** → **Kaspersky CyberTrace** Консоли OSMP.

Чтобы интегрировать веб-интерфейс CyberTrace в Консоль OSMP:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Создать**, чтобы создать новый секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу CyberTrace.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип** выберите **credentials**.

   d. В полях **Пользователь** и **Пароль** введите учетные данные для вашего сервера CyberTrace.

   e. При необходимости в раскрывающемся списке **Теги** выберите теги для секрета.

   f. При необходимости в поле **Описание** добавьте до 4000 символов Юникода.

4. Нажмите на кнопку **Создать**.

   Учетные данные сервера CyberTrace сохранены и могут использоваться в других ресурсах KUMA.

5. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

6. В разделе **Анализ угроз** нажмите **Kaspersky CyberTrace**.

   Откроется окно **Интеграция с Kaspersky CyberTrace**.

7. Измените необходимые параметры:

   - **Состояние** – включите переключатель, если хотите интегрировать веб-интерфейс CyberTrace в Консоль OSMP.
   - **Адрес сервера** (обязательно) – введите адрес сервера CyberTrace.
   - **Порт** (обязательно) – введите порт сервера CyberTrace, порт для доступа к веб-интерфейсу по умолчанию 443.
   - В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.
   - **Разрешить хосты** – в раскрывающемся списке выберите устройства, для которых поддерживается технология CORS.
   - **Основная версия CyberTrace** – выберите версию CyberTrace. Доступные значения: **<5**, **≥ 5.0**. При выборе версии **≥ 5.0** запросы будут выполняться в тенанте General в CyberTrace и будут использовать новую версию API, соответствующую Kaspersky CyberTrace 5.0 и выше. При выборе значения **<5** запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: **<5**.

8. Вы можете настроить доступ к веб-интерфейсу CyberTrace следующими способами:

   - Использовать hostname или IP при входе в Консоль OSMP.

     Для этого в разделе **Разрешить хосты** нажмите **Добавить хост** и в появившемся поле укажите IP или hostname устройства.

- Использовать FQDN при входе в Консоль OSMP.

  Если для работы в Консоли вы используете браузер Mozilla Firefox, данные в разделе CyberTrace могут не отображаться. В таком случае настройте отображение данных (см. ниже).

9. Нажмите на кнопку **Сохранить**.

CyberTrace теперь интегрирован с OSMP: раздел **CyberTrace** отображается в Консоли OSMP.

*Чтобы настроить отображение данных в разделе **CyberTrace** при использовании FQDN для входа в Консоль OSMP в Mozilla Firefox:*

1. Очистите кеш браузера.

2. В строке браузера введите FQDN Консоли OSMP с номером порта.

   Отобразится окно с предупреждением о вероятной угрозе безопасности.

3. Нажмите на кнопку **Подробнее**.

4. В нижней части окна нажмите на кнопку **Принять риск и продолжить**.

   Для URL Консоли OSMP будет создано исключение.

5. В строке браузера введите URL Консоли OSMP с номером порта.

6. Перейдите в раздел **CyberTrace**.

Данные отобразятся в разделе.

Обновление списка запрещенных объектов CyberTrace (Internal TI)

Если веб-интерфейс CyberTrace интегрирован в Консоль OSMP, можно обновлять список запрещенных объектов CyberTrace или **Internal TI** данными из событий KUMA.

Чтобы обновить Internal TI в CyberTrace:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   Откроется контекстное меню.

2. Выберите **Добавить в Internal TI CyberTrace**.

Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

Подключение по протоколу LDAP

LDAP-подключения создаются и управляются в разделе **Настройки** → **KUMA** → **Открыть параметры KUMA** → **LDAP-сервер** в Консоли OSMP. В разделе **Интеграция с LDAP-сервером по тенантам** отображаются тенанты, для которых созданы подключения по протоколу LDAP. Тенанты можно создать или удалить.

Если выбрать тенант, откроется окно **Интеграция с LDAP-сервером**, в котором отображается таблица с существующими LDAP-подключениями. Подключения можно создать или изменить. В этом же окне можно изменить частоту обращения к LDAP-серверам и установить срок хранения устаревших данных.

После включения интеграции информация об учетных записях Active Directory становится доступной в окне алертов, в окне с подробной информацией о корреляционных событиях, а также окне инцидентов. При выборе имени учетной записи в разделе **Связанные пользователи** откроется окно **Информация об учетной записи** с данными, импортированными из Active Directory.

Данные из LDAP можно также использовать при обогащении событий в коллекторах и в аналитике.

Импортируемые атрибуты Active Directory

Из Active Directory можно запросить следующие атрибуты учетных записей:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `co`
- `company`
- `department`
- `description`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `givenName`
- `l`
- `lastLogon`
- `lastLogonTimestamp`
- `Mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)

- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSID`
- `physicalDeliveryOfficeName`
- `pwdLastSet`
- `sAMAccountName`
- `sAMAccountType`
- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `UserPrincipalName`
- `whenChanged`
- `whenCreated`

Подробнее об атрибутах Active Directory см. в документации Microsoft.

Включение и выключение LDAP-интеграции

Можно включить или выключить сразу все LDAP-подключения тенанта, а можно включить или выключить только определенное LDAP-подключение.

Чтобы включить или отключить все LDAP-подключения тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**, а затем выберите тенант, для которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

3. Включите или отключите переключатель **Состояние**.

4. Нажмите на кнопку **Сохранить**.

Чтобы включить или отключить определенное LDAP-подключение:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**, а затем выберите тенант, для которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

3. В таблице подключений включите или выключите переключатель **Состояние** для соответствующего подключения.

4. Нажмите на кнопку **Сохранить**.

Добавление тенанта в список тенантов для интеграции с LDAP-сервером

Чтобы добавить тенант в список тенантов для интеграции с LDAP-сервером:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Нажмите на кнопку **Добавить параметры для нового тенанта**.

   Отобразится окно **Интеграция с LDAP-сервером**.

4. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.

5. Нажмите на кнопку **Сохранить**.

Выбранный тенант добавлен в список тенантов для интеграции с LDAP-сервером.

Чтобы добавить тенант из списка тенантов для интеграции с LDAP-сервером:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Установите флажок рядом с тенантом, который необходимо удалить, и нажмите на кнопку **Удалить**.

4. Подтвердите удаление тенанта.

Выбранный тенант удален из списка тенантов для интеграции с LDAP-сервером.

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите или создайте тенант, для которого хотите создать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Нажмите на кнопку **Добавить подключение**.

   Откроется окно **Параметры подключения**.

5. Добавьте секрет с учетными данными для подключения к серверу Active Directory. Для этого выполните следующие действия:

   a. Если вы добавили секрет ранее, в раскрывающемся списке **Секрет** выберите существующий секрет типа **credentials**.

      Выбранный секрет можно изменить, нажав на значок карандаша ( ).

   b. Если вы хотите создать секрет, нажмите на значок плюса ( ).

      Откроется окно **Секрет**.

   c. В поле **Название** (обязательно) введите название секрета: от 1 до 128 символов Юникода.

   d. В полях **Пользователь** и **Пароль** (обязательно) введите учетные данные для подключения к серверу Active Directory.

      Вы можете указать имя пользователя в одном из следующих форматов: <имя пользователя>@<домен> или <домен><имя пользователя>.

   e. В поле **Описание** введите описание до 4000 символов Юникода.

   f. Нажмите на кнопку **Сохранить**.

6. В поле **Название** (обязательно) введите уникальное имя LDAP-подключения.

   Длина должна быть от 1 до 128 символов Юникода.

7. В поле **URL** (обязательно) введите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

   Вы можете указать через запятую адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

8. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Тип** выберите один из следующих вариантов:

   - **startTLS**.

     При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается.

     > Убедитесь, что порт 389 открыт. В противном случае соединение с контроллером домена будет невозможно.

   - **ssl**.

     При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

9. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Для этого выполните следующие действия:

   a. Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Сертификат**.

      Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

   b. Если вы хотите загрузить новый сертификат, справа от списка **Сертификат** нажмите на значок плюса (+).

      Откроется окно **Секрет**.

   c. В поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления.

   d. По кнопке **Загрузить файл сертификата** добавьте файл с сертификатом Active Directory. Поддерживаются открытые ключи сертификата X.509 в Base64.

   e. Если требуется, укажите любую информацию о сертификате в поле **Описание**.

   f. Нажмите на кнопку **Сохранить**.

   Сертификат будет загружен и отобразится в списке **Сертификат**.

10. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

    Если в поле **URL** указано несколько адресов, KUMA будет ожидать ответа от первого сервера указанное количество секунд. Если в течение этого времени не будет получено никакого ответа, приложение свяжется со следующим сервером. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

11. В поле **Base DN** введите базовое отличительное имя директории, в которой должен выполняться поисковый запрос.

12. В поле **Пользовательские атрибуты учетных записей AD** укажите **дополнительные атрибуты, с использованием которых вы хотите обогащать события**.

    Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

    Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

    1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

       Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартный атрибут `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

       Из Active Directory можно запросить следующие атрибуты учетных записей:

       - `accountExpires`
       - `badPasswordTime`
       - `cn`
       - `co`
       - `company`
       - `department`
       - `description`
       - `displayName`
       - `distinguishedName`
       - `division`
       - `employeeID`
       - `givenName`
       - `l`
       - `lastLogon`
       - `lastLogonTimestamp`
       - `Mail`
       - `mailNickname`
       - `managedObjects`
       - `manager`
       - `memberOf` (по этому атрибуту события можно искать при корреляции)

- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSID`
- `physicalDeliveryOfficeName`
- `pwdLastSet`
- `sAMAccountName`
- `sAMAccountType`
- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `UserPrincipalName`
- `whenChanged`
- `whenCreated`

После того как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если вы добавили один и тот же атрибут для нескольких доменов, атрибут отображается в раскрывающемся списке только один раз. Вы можете просмотреть домены, наведя курсор на вопросительный знак. Названия доменов отображаются в виде ссылок. Если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.

3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.

4. Перезапустите коллектор.

   После перезапуска коллектора KUMA начнет обогащать события учетными записями.

13. Установите флажок **Выключено**, если не хотите использовать это LDAP-подключение.

    По умолчанию флажок снят.

14. Нажмите на кнопку **Сохранить**.

LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером по тенантам**.

Информация об учетных записях из Active Directory будет запрошена сразу после сохранения подключения, а затем будет обновляться с указанной периодичностью.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Создание копии подключения к LDAP-серверу

Вы можете создать LDAP-подключение, скопировав уже существующее подключение. В этом случае в созданное подключение дублируются все параметры исходного подключения.

Чтобы скопировать LDAP-подключение:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите тенант, для которого вы хотите скопировать подключение к LDAP-серверу.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Выберите нужное подключение.

5. В открывшемся окне **Параметры подключения** нажмите на кнопку **Дублировать подключение**.

   Отобразится окно создания нового подключения. К названию подключения будет добавлено слово `копия`.

6. Если требуется, измените нужные параметры.

7. Нажмите на кнопку **Сохранить**.

Создано новое подключение.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Изменение подключения к LDAP-серверу

Чтобы изменить подключение к LDAP-серверу:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите тенант, для которого вы хотите изменить подключение к LDAP-серверу.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Нажмите на подключение с LDAP-серверу, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к LDAP-серверу.

5. Измените значения необходимых параметров.

6. Нажмите на кнопку **Сохранить**.

Подключение к LDAP-серверу изменено. Перезапустите сервисы KUMA, использующие обогащение данными LDAP-серверов, чтобы изменения вступили в силу.

Изменение периода обновления данных

KUMA обращается к LDAP-серверу для обновления данных об учетных записях. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов.
- При создании пользователем задачи на обновление данных об учетных записях.

При обращении к LDAP-серверам создается задача в Консоли KUMA в разделе **Диспетчер задач**.

Чтобы изменить расписание обращений KUMA к LDAP-серверам:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

4. В поле **Период обновления данных** укажите требуемую частоту в часах. По умолчанию указано значение 12.

Расписание обращений изменено.

Изменение срока хранения данных

Полученные данные об учетных записях, если сведения о них перестают поступать от сервера Active Directory, по умолчанию хранятся в KUMA в течение 90 дней. По прошествии этого срока данные удаляются.

После удаления данных об учетных записях в KUMA новые и существующие события не обогащаются этой информацией. Информация об учетных записях также будет недоступна в алертах. Если вы хотите просматривать информацию об учетных записях на протяжении всего времени хранения алерта, требуется установить срок хранения данных об учетных записях больше, чем срок хранения алерта.

Чтобы изменить срок хранения данных об учетных записях:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

4. В поле **Время хранения данных** укажите количество дней, в течение которого требуется хранить полученные от LDAP-сервера данные.

Срок хранения данных об учетных записях изменен.

Запуск задач на обновление данных об учетных записях

После создания подключения к серверу Active Directory задачи на получение данных об учетных записях создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную. Загрузить данные можно для всех подключений требуемого тенанта, так и для одного подключения.

Чтобы запустить задачу на обновление данных об учетных записях для всех LDAP-подключений тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Нажмите на кнопку **Импортировать учетные записи**.

В Консоли KUMA в разделе **Диспетчер задач** добавлена задача на получение данных об учетных записях выбранного тенанта.

Чтобы запустить задачу на обновление данных об учетных записях для одного LDAP-подключения тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Выберите требуемое подключение к LDAP-серверу.

   Откроется окно **Параметры подключения**.

5. Нажмите на кнопку **Импортировать учетные записи**.

В Консоли KUMA в разделе Диспетчер задач добавлена **задача** на получение данных об учетных записях из выбранного подключения тенанта.

Удаление подключения к LDAP-серверу

Чтобы удалить LDAP-подключения к Active Directory:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Интеграции** нажмите **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Выберите тенант, которому принадлежит соответствующее LDAP-подключение.

   Откроется окно **Интеграция с LDAP-сервером**.

4. Нажмите на подключение LDAP, которое вы хотите удалить, а затем нажмите на кнопку **Удалить**.

5. Подтвердите удаление подключения.

   LDAP-подключение к Active Directory удалено.

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks (далее "KICS for Networks") – программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Приложение анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

KICS for Networks версии 4.0 и выше можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Импортировать из KICS for Networks в KUMA сведения об активах.
- Отправлять из KUMA в KICS for Networks команды на изменение статусов активов.

> В отличие от KUMA, в KICS for Networks активы называются устройствами.

Интеграцию KICS for Networks и KUMA необходимо настроить на стороне обоих приложений:

1. В KICS for Networks необходимо создать коннектор KUMA и сохранить файл свертки этого коннектора.
2. В KUMA с помощью файла свертки коннектора создается подключение к KICS for Networks.

> Описываемая в этом разделе интеграция касается импорта сведений об активах. KICS for Networks можно также настроить на отправку событий в KUMA. Для этого необходимо в KICS for Networks создать коннектор типа SIEM/syslog, а на стороне KUMA – настроить коллектор.

Настройка интеграции в KICS for Networks

> Интеграция поддерживается с KICS for Networks версий 4.0 и выше.

> Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

На стороне KICS for Networks настройка интеграции заключается в создании *коннектора типа KUMA*. В KICS for Networks коннекторы – это специальные модули приложений, которые обеспечивают обмен данными KICS for Networks со сторонними системами, в том числе с KUMA. Подробнее о создании коннекторов см. в документации KICS for Networks.

При добавлении в KICS for Networks коннектора автоматически создается *файл свертки* для этого коннектора. Это зашифрованный файл конфигурации для подключения к KICS for Networks, который используется при настройке интеграции на стороне KUMA.

Настройка интеграции в KUMA

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

Чтобы настроить в KUMA интеграцию с KICS for Networks:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого хотите создать интеграцию с KICS for Networks.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Параметры активов**.
4. На вкладке **Импорт KICS/KATA** нажмите на кнопку **Добавить**.
5. Откроется окно **Создать подключения**.
6. Чтобы включить или отключить подключение, включите или выключите переключатель **Состояние**.
7. Нажмите на значок "плюс" (+) и выберите файл свертки коннектора, созданный в KICS for Networks.
8. В поле **Пароль файла свертки** введите пароль файла свертки.
9. В поле **Версия API** введите версию API KICS/KATA, которая будет использоваться для связи с KICS/KATA. По умолчанию используется версия 4.
10. Нажмите на кнопку **Добавить**.
11. Установите флажок **Включить действия по реагированию**, если вы хотите изменять статусы активов KICS for Networks с помощью правил реагирования KUMA.
12. Нажмите на кнопку **Сохранить**.

В KUMA настроена интеграция с KICS for Networks, в окне отображается IP-адрес узла, на котором будет работать коннектор KICS for Networks, а также его идентификатор.

Включение и выключение интеграции с KICS for Networks

Чтобы включить или выключить для тенанта интеграцию с KICS for Networks:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите импортировать активы KICS/KATA.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Параметры активов**.

4. На вкладке **Импорт KICS/KATA** включите или выключите переключатель **Состояние**.

5. Нажмите на кнопку **Сохранить**.

Изменение периода обновления данных

KUMA обращается к KICS for Networks для обновления сведений об активах. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 3 часа.
- При создании пользователем задачи на обновление данных об активах.

При обращении к KICS for Networks создается задача в Консоли OSMP в разделе **Диспетчер задач**.

Чтобы изменить расписание импорта сведений об активах KICS for Networks:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите импортировать активы KICS/KATA.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Параметры активов**.
4. На закладке **Импорт KICS/KATA** в поле **Интервал импорта (в часах)** укажите интервал, через который OSMP будет обновлять данные об активах KICS/KATA.

Расписание импорта изменено.

Особенности импорта информации об активах из KICS for Networks

Импорт активов

Активы импортируются в соответствии с правилами импорта активов. Импортируются только активы со статусами **Разрешенное** и **Неразрешенное**.

Активы KICS for Networks идентифицируются по комбинации следующих параметров:

- IP-адрес экземпляра KICS for Networks, с которым настроена интеграция.
- Идентификатор коннектора KICS for Networks, с помощью которого настроена интеграция.
- Идентификатор, присвоенный активу (или "устройству") в экземпляре KICS for Networks.

Импорт сведений об уязвимостях

При импорте активов в KUMA также поступают сведения об активных уязвимостях KICS for Networks. Если в KICS for Networks уязвимость была помечена как устраненная или незначительная, сведения о ней удаляются из KUMA при следующем импорте.

Сведения об уязвимостях активов отображаются в окне **Информация об активе** в блоке параметров **Уязвимости** на языке локализации KICS for Networks.

> В KICS for Networks уязвимости называются рисками и разделяются на несколько типов. В KUMA импортируются все типы рисков.

Срок хранения импортированных данных

Если сведения о ранее импортированном активе перестают поступать из KICS for Networks, актив удаляется по прошествии 30 дней.

Изменение статуса актива KICS for Networks

После настройки интеграции вы можете менять статусы активов KICS for Networks из KUMA. Статусы можно менять автоматически и вручную.

Статусы активов можно менять, только если вы включили реагирование в настройках подключения к KICS for Networks.

Изменение статуса актива KICS for Networks вручную

Пользователи с ролями Главный администратор, Администратор и Аналитик в доступных им тенантах могут вручную менять статусы активов, импортированных из KICS for Networks.

Чтобы вручную изменить статус актива KICS for Networks:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.
2. Нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.
3. В раскрывающемся списке **Статус KICS for Networks** выберите статус, который необходимо присвоить активу KICS for Networks. Доступны статусы *Разрешенное* или *Неразрешенное*.

Статус актива изменен. Новый статус отображается в KICS for Networks и в KUMA.

Изменение статуса актива KICS for Networks автоматически

Автоматическое изменение статусов активов KICS for Networks реализовано с помощью правил реагирования. Правила необходимо добавить в коррелятор, который будет определять условия их срабатывания.

Интеграция с Neurodat SIEM IM

Система Neurodat SIEM IM предназначена для мониторинга информационной безопасности.

Вы можете настроить передачу событий KUMA в Neurodat SIEM IM. На основе поступающих событий и правил корреляции в системе Neurodat SIEM IM автоматически формируются инциденты информационной безопасности.

Чтобы настроить интеграцию с Neurodat SIEM IM:

1. Подключитесь к серверу Neurodat SIEM IM по протоколу SSH под учетной записью с административными привилегиями.

2. Создайте резервную копию конфигурационного файла /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties.

3. В конфигурационном файле /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties установите указанные значения для следующих параметров:

   - `kuma.on=true`

     Этот параметр является признаком взаимодействия с Neurodat SIEM IM с KUMA.

   - `job_kuma=com.cbi.soz.server.utils.scheduler.KumaIncidentsJob`

   - `jobDelay_kuma=5000`

   - `jobPeriod_kuma=60000`

4. Сохраните изменения конфигурационного файла.

5. Перезапустите службу tomcat с помощью команды:

   ```
   sudo systemctl restart tomcat
   ```

6. Получите токен для пользователя в KUMA. Для этого выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **Параметры** → **API-токены**.

      Откроется окно **API-токены**.

   b. Нажмите на кнопку **Добавить токен**.

      Откроется окно **Добавить токен**.

c. Если требуется, установите срок действия токена:

- Установите флажок **Срок действия не ограничен**.
- В поле **Срок действия** с помощью календаря укажите дату и время истечения срока действия создаваемого токена.

d. Нажмите на кнопку **Сгенерировать**.

В области деталей пользователя отобразится поле **Токен** с автоматически созданным токеном. Скопируйте его.

При закрытии окна токен больше не отображается. Если вы не скопировали токен перед закрытием окна, вам нужно будет сгенерировать новый токен.

e. Нажмите на кнопку **Сохранить**.

7. Войдите в Neurodat SIEM IM под учетной записью admin или другой учетной записью, обладающей ролью Администратор для настраиваемой организации или Администратор всех организаций.

8. В пункте меню **Администрирование** → **Структура организации** выберите или создайте организацию, которая будет получать инциденты из KUMA.

9. На форме организации выполните следующие действия:

   a. Установите флажок **Настроить интеграцию с KUMA**.

   b. В поле **IP адрес и сетевой порт KUMA** укажите адрес API KUMA, например `https://192.168.58.27:7223/api/v1/`.

   c. В поле **Ключ API KUMA** укажите токен пользователя, полученный на шаге 6.

   d. Сохраните данные организации.

Настройка интеграции с KUMA будет завершена.

Neurodat SIEM IM выполнит проверку доступа к KUMA и в случае успеха отобразит сообщение о готовности получать данные из KUMA.

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также "KASAP") – это платформа для онлайн-обучения, с помощью которой пользователи смогут усвоить правила соблюдения информационной безопасности, узнать о связанных с ней угрозах, подстерегающих их в ежедневной деятельности, и потренироваться на практических примерах.

Платформу KASAP можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Изменять группы обучения пользователей.
- Просматривать информацию о курсах, пройденных пользователями, и полученных ими сертификатах.

Интеграция KASAP и KUMA заключается в настройке API-подключения к платформе KASAP. Процесс происходит в обоих продуктах:

1. В KASAP необходимо создать токен для авторизации API-запросов и получить адрес для API-запросов.
2. В KUMA необходимо указать адрес для API-запросов в KASAP, добавить токен для авторизации API-запросов, а также указать адрес электронной почты администратора KASAP для получения уведомлений.

Создание токена в KASAP и получение ссылки для API-запросов

Для авторизации API-запросов из KUMA в KASAP их необходимо подписывать токеном, созданном в платформе KASAP. Только администраторы компании могут создать токены.

Создание токена

Чтобы создать токен:

1. Войдите в веб-интерфейс KASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.
3. Нажмите на кнопку **Новый токен** и в открывшемся окне выберите методы API, используемые при интеграции:
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
4. Нажмите на кнопку **Сгенерировать токен**.
5. Скопируйте токен и сохраните его любым удобным способом. Этот токен необходим для настройки интеграции в KUMA.

> Токен не хранится в системе KASAP в открытом виде. После закрытия окна **Получить токен** он становится недоступным для просмотра. Если вы закрыли это окно, не скопировав токен, вам требуется нажать на кнопку **Новый токен** повторно, чтобы система сгенерировала новый токен.

Выданный токен действителен 12 месяцев. По истечении этого срока токен будет отозван. Выпущенный токен будет также отозван, если он не используется в течении 6 месяцев.

Получение ссылки для API-запросов

Чтобы получить ссылку, используемую в KASAP для API-запросов:

1. Войдите в консоль платформы KASAP.

2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.

3. Ссылка для обращения к KASAP через Open API расположена в нижней части окна. Скопируйте ссылку и сохраните ее любым удобным способом. Эта ссылка необходима для настройки интеграции в KUMA.

Настройка интеграции в KUMA

Чтобы настроить в KUMA интеграцию с KASAP:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно **Параметры KUMA**.

2. В разделе **Интеграции** нажмите **Kaspersky Automated Security Awareness Platform**.

   Откроется окно **Интеграция с Kaspersky Automated Security Awareness Platform**.

3. В поле **Секрет** с помощью значка плюса (+) создайте секрет типа **token**, указав в нем токен, полученный в платформе KASAP:

   a. В поле **Название** введите название для секрета. Имя должно содержать от 1 до 128 символов Юникода.

   b. В поле **Токен** введите токен для авторизации API-запросов в KASAP.

   c. При необходимости добавьте описание секрета в поле **Описание**.

   d. Нажмите на кнопку **Сохранить**.

4. В поле **URL для OpenAPI KASAP** укажите адрес, используемый платформой KASAP для API-запросов.

5. В поле **Адрес электронной почты администратора KASAP** укажите адрес электронной почты администратора KASAP, который должен получать уведомления при добавлении пользователей в группы обучения через KUMA.

6. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который следует использовать для подключения к платформе KASAP.

7. При необходимости выключить или включить интеграцию с KASAP установите или снимите флажок **Выключено**.

8. Нажмите на кнопку **Сохранить**.

В KUMA настроена интеграция с KASAP. Теперь при просмотре информации об алертах и инцидентах можно выбрать относящихся к ним пользователей, чтобы просмотреть, какие курсы обучения прошли пользователи, а также изменить их группу обучения.

Просмотр данных о пользователях KASAP и изменение учебных групп

После настройки интеграции KASAP и KUMA в алертах и инцидентах при просмотре данных о связанных с ними пользователях становятся доступны данные из KASAP:

- Учебная группа, к которой принадлежит пользователь.
- Сведения о пройденных курсах.
- Сведения о запланированном обучении и текущем прогрессе.
- Сведения о полученных сертификатах.

Чтобы просмотреть данные о пользователе из KASAP:

1. В Консоли OSMP в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.
2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.
3. Выберите вкладку **Данные о курсах KASAP**.

В окне отображаются данные пользователя из KASAP.

Вы можете изменить учебную группу пользователя KASAP.

Чтобы изменить учебную группу KASAP:

1. В Консоли OSMP в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.
2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.
3. В раскрывающемся списке **Присвоить пользователю группу KASAP** выберите учебную группу KASAP, в которую вы хотите поместить пользователя.
4. Нажмите **Применить**.

Пользователь будет перемещен в выбранную группу KASAP, администратор компании платформы KASAP получит уведомление об изменении состава учебных групп, а для выбранной учебной группы начнет пересчитываться учебный план.

Подробнее об учебных группах и начале обучения см. в документации KASAP.

Отправка уведомлений в Telegram

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить отправку уведомлений в Telegram о срабатывании правил корреляции KUMA. Это позволит уменьшить время реакции на угрозы и при необходимости расширить круг информированных лиц.

Настройка отправки уведомлений в Telegram состоит из следующих этапов:

1. Создание и настройка бота в Telegram

   Уведомления о срабатывании правил корреляции отправляет специально созданный бот. Он может отправлять уведомления в личный или групповой чат Telegram.

2. Создание скрипта для отправки уведомлений

   Вам необходимо создать скрипт и сохранить его на сервере, где установлен коррелятор.

3. Настройка отправки уведомлений в KUMA

   Настройте правило реагирования KUMA, запускающее скрипт для отправки уведомлений, и добавьте это правило в коррелятор.

Создание и настройка бота в Telegram

Чтобы создать и настроить бот в Telegram:

1. В приложении Telegram найдите бот BotFather и откройте чат с ним.

2. В чате нажмите на кнопку **Старт**.

3. Создайте новый бот при помощи команды:

   ```
   /newbot
   ```

4. Введите имя бота.

5. Введите логин бота.

   Бот будет создан. Вы получите ссылку на чат вида t.me/<логин бота> и токен для обращения к боту.

6. Если вы хотите использовать бота в групповом чате, а не в личных сообщениях, необходимо изменить параметры приватности:

   a. В чате бота BotFather введите команду:

   ```
   /mybots
   ```

   b. Выберите нужный бот из списка.

c. Нажмите **Bot Settings** → **Group Privacy** и выберите параметр **Turn off**.

Бот сможет отправлять сообщения в групповые чаты.

7. Откройте чат с созданным ботом по ссылке вида t.me/<логин бота>, полученной на шаге 5, и нажмите на кнопку **Старт**.

8. Если вы хотите, чтобы бот отправлял личные сообщения пользователю:

   a. В чате с созданным ботом отправьте произвольное сообщение.

   b. Перейдите по ссылке https://t.me/getmyid_bot и нажмите на кнопку **Старт**.

   c. В ответе вы получите значение `Current chat ID`. Это значение понадобится при настройке отправки сообщений.

9. Если вы хотите, чтобы бот отправлял сообщения в групповой чат:

   a. Добавьте бот https://t.me/getmyid_bot в групповой чат, предназначенный для получения уведомлений от KUMA.

   Бот пришлет в групповой чат сообщение, в котором будет указано значение `Current chat ID`. Это значение понадобится при настройке отправки сообщений.

   b. Удалите бот из группы.

10. Отправьте тестовое сообщение через бот. Для этого в адресную строку браузера вставьте следующую ссылку:

    `https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test`

    где `<token>` – значение, полученное на шаге 5, `<chat_id>` – значение, полученное на шаге 8 или 9.

В результате в личном или групповом чате должно появиться тестовое сообщение, а в ответе браузера JSON не должен содержать ошибок.

Создание скрипта для отправки уведомлений

Чтобы создать скрипт:

1. В консоли сервера, на котором установлен коррелятор, создайте файл скрипта и добавьте в него следующие строки:

```
#!/bin/bash
set -eu
CHAT_ID=<значение Current chat ID, полученное на шаге 8 или 9 инструкции по настройке бота Telegram>
TG_TOKEN=<значение токена, полученное на шаге 5 инструкции по настройке бота Telegram>
RULE=$1
TEXT="Сработало правило <b>$RULE</b>"
curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

   Если на сервере коррелятора нет доступа к интернету, вы можете использовать прокси-сервер:

```
#!/bin/bash
set -eu
CHAT_ID=<значение Current chat ID, полученное на шаге 8 или 9 инструкции по настройке бота Telegram>
```

```
TG_TOKEN=<значение токена, полученное на шаге 5 инструкции по настройке бота Telegram>
RULE=$1
TEXT="Сработало правило <b>$RULE</b>"
PROXY=<адрес и порт прокси-сервера>
curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT"
--data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

2. Сохраните скрипт в директорию коррелятора, расположенную по пути /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет реагировать на события>/scripts/.

   Информацию о том, как узнать ID коррелятора, см. в разделе Получение идентификатора сервиса.

3. Назначьте пользователя kuma владельцем файла и дайте права на исполнение при помощи следующих команд:

```
chown kuma:kuma /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет реагировать>/scripts/<имя скрипта>.sh
chmod +x /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет реагировать>/scripts/<имя скрипта>.sh
```

Настройка отправки уведомлений в KUMA

Чтобы настроить отправку уведомлений KUMA в Telegram:

1. Создайте правило реагирования:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила реагирования** и нажмите **Добавить правило реагирования**.

   b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

   c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

   e. В поле **Название скрипта** укажите имя скрипта.

   f. В поле **Аргументы скрипта** укажите `{{.Name}}`.

      В качестве аргумента выполнения скрипта будет передаваться имя корреляционного события.

   g. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

   a. В главном меню перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы** и выберите коррелятор, в папку которого вы поместили созданный скрипт для отправки уведомлений.

   b. В дереве шагов выберите **Правила реагирования**.

   c. Нажмите на кнопку **Добавить**.

   d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

e. В дереве шагов выберите **Проверка параметров**.

f. Нажмите на кнопку **Сохранить и перезапустить службы**.

g. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о срабатывании правил KUMA в Telegram будет настроена.

Интеграция с UserGate

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

UserGate – решение, которое обеспечивает безопасность сетевой инфраструктуры, позволяет защитить персональные данные от рисков, связанных с внешними вторжениями, несанкционированным доступом, вирусами и вредоносными приложениями.

Интеграция с UserGate позволяет настроить автоматическую блокировку угроз по IP-адресу, URL или доменному имени при срабатывании правил реагирования KUMA.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в UserGate
2. Подготовка скрипта для правила реагирования
3. Настройка правила реагирования KUMA

Настройка интеграции в UserGate

Чтобы настроить интеграцию в UserGate:

1. Подключитесь к веб-интерфейсу UserGate под учетной записью администратора.
2. Перейдите в раздел **UserGate** → **Администраторы** → **Профили администраторов** и нажмите **Добавить**.
3. В окне **Настройка профиля** укажите имя профиля, например `API`.
4. На вкладке **Разрешения для API** добавьте разрешения на чтение и запись для следующих объектов:
   - content
   - core
   - firewall
   - nlists

5. Нажмите на кнопку **Сохранить**.

6. В разделе **UserGate** → **Администраторы** нажмите **Добавить** → **Добавить локального администратора**.

7. В окне **Свойства администратора** укажите логин и пароль администратора.

   В поле **Профиль администратора** выберите профиль, созданный на шаге 3.

8. Нажмите на кнопку **Сохранить**.

9. В адресной строке браузера после адреса и порта UserGate допишите `?features=zone-xml-rpc` и нажмите **ENTER**.

10. Перейдите в раздел **Сеть** → **Зоны** и для зоны того интерфейса, через который будет осуществляться взаимодействие по API, перейдите на вкладку **Контроль доступа** и установите флажок рядом с сервисом **XML-RPC для управления**.

    В список разрешенных адресов при необходимости можно добавить IP-адрес коррелятора KUMA, по правилам корреляции которого должна срабатывать блокировка в UserGate.

11. Нажмите на кнопку **Сохранить**.

Подготовка скрипта для интеграции с UserGate

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка URL, IP-адреса или доменного имени в UserGate:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

   b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

      Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Откройте файл скрипта и в блоке **Enter UserGate Parameters** в параметрах **login** и **password** укажите данные учетной записи администратора UserGate, которая была создана на шаге 7 настройки интеграции в UserGate.

4. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<`ID коррелятора из шага 1`>/scripts/.

5. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 4 при помощи команды:

   ```
   cd /opt/kaspersky/kuma/correlator/< ID коррелятора из шага 1 >/scripts/
   ```

6. Выполните следующую команду:

   ```
   chmod +x ug.py && chown kuma:kuma ug.py
   ```

Скрипт будет готов к использованию.

Настройка правила реагирования для интеграции с UserGate

Чтобы настроить правило реагирования:

1. Создайте правило реагирования:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила реагирования** и нажмите **Добавить правило реагирования**.

   b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

   c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

   e. В поле **Название скрипта** укажите имя скрипта. `ug.py`.

   f. В поле **Аргументы скрипта** укажите:

      - одну из операций в соответствии с типом блокируемого объекта:

        - `blockurl` – заблокировать доступ по URL;

        - `blockip` – заблокировать доступ по IP-адресу;

        - `blockdomain` – заблокировать доступ по доменному имени.

      - `-i {{< поле KUMA, из которого будет взято значение блокируемого объекта, в зависимости от операции >}}`

        Пример:
        `blockurl -i {{.RequetstUrl}}`

   g. В блоке **Условия** добавьте условия, соответствующие правилам корреляции, при срабатывании которых необходима блокировка в UserGate.

   h. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы** и выберите коррелятор, который должен отвечать и в директорию которого вы поместили скрипт.

   b. В дереве шагов выберите **Правила реагирования**.

   c. Нажмите на кнопку **Добавить**.

   d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

   e. В дереве шагов выберите **Проверка параметров**.

f. Нажмите на кнопку **Сохранить и обновить параметры служб**.

g. Нажмите на кнопку **Сохранить**.

Правило реагирования будет привязано к коррелятору и готово к использованию.

Интеграция с Kaspersky Web Traffic Security

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить интеграцию с системой анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (далее также "KWTS").

Настройка интеграции заключается в создании правил реагирования KUMA, которые позволяют запускать задачи KWTS. Задачи должны быть предварительно созданы в веб-интерфейсе KWTS.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в KWTS
2. Подготовка скрипта для правила реагирования
3. Настройка правила реагирования KUMA

Настройка интеграции в KWTS

Чтобы подготовиться к интеграции в KWTS:

1. Подключитесь к веб-интерфейсу KWTS под учетной записью администратора и создайте роль с правами на просмотр и создание/изменение правила.

   Подробнее о создании роли см. *справку Kaspersky Web Traffic Security*.

2. Назначьте созданную роль пользователю с NTML-аутентификацией.

   Вместо этого вы можете использовать учетную запись локального администратора.

3. В разделе **Правила** перейдите на вкладку **Доступ** и нажмите **Добавить правило**.

4. В раскрывающемся списке **Действие** выберите **Заблокировать**.

5. В раскрывающемся списке **Фильтрация трафика** выберите значение **URL** и в поле справа укажите несуществующий или заведомо вредоносный адрес.

6. В поле **Название правила** укажите название правила.

7. Включите использование правила с помощью переключателя **Статус**.

8. Нажмите на кнопку **Добавить**.

9. В веб-интерфейсе KWTS откройте только что созданное правило.

10. Запишите значение ID, отображаемое в конце адреса страницы в адресной строке браузера.

    Это значение будет использовано при настройке правила реагирования в KUMA.

Подготовка к интеграции в KWTS будет завершена.

Подготовка скрипта для интеграции с KWTS

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка URL, IP-адреса или доменного имени в KWTS:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

   b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

      Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт и библиотеку по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<`ID коррелятора из шага 1`>/scripts/.

4. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 3 при помощи команды:

   ```
   cd /opt/kaspersky/kuma/correlator/< ID коррелятора из шага 1 >/scripts/
   ```

5. Выполните следующую команду:

   ```
   chmod +x kwts.py kwtsWebApiV6.py && chown kuma:kuma kwts.py kwtsWebApiV6.py
   ```

Скрипт будет готов к использованию.

Настройка правила реагирования для интеграции с KWTS

Чтобы настроить правило реагирования:

1. Создайте правило реагирования:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила реагирования** и нажмите **Добавить правило реагирования**.

   b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

   c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

e. В поле **Название скрипта** укажите имя скрипта. kwts.py.

f. В поле **Аргументы скрипта** укажите:

- `--host` – адрес сервера KWTS.
- `--username` – имя учетной записи пользователя, созданной в KWTS, или локального администратора.
- `--password` – пароль учетной записи пользователя KWTS.
- `--rule_id` – ID правила, созданного в KWTS.
- Укажите один из ключей в соответствии с типом блокируемого объекта:
  - `--url` – укажите поле события KUMA, из которого вы хотите получать URL, например `{{.RequestUrl}}`.
  - `--ip` – укажите поле события KUMA, из которого вы хотите получать IP-адрес, например `{{.DestinationAddress}}`.
  - `--domain` – укажите поле события KUMA, из которого вы хотите получать доменное имя, например `{{.DestinationHostName}}`.
- `--ntlm` – укажите этот ключ, если пользователь KWTS был создан с NTLM-аутентификацией.

Пример:
```
--host <address> --username <user> --password <pass> --rule_id <id> --url {{.RequestUrl}}
```

g. В блоке **Условия** добавьте условия, соответствующие правилам корреляции, по срабатыванию которых необходима блокировка в KWTS.

h. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы** и выберите коррелятор, который должен отвечать и в директорию которого вы поместили скрипт.

b. В дереве шагов выберите **Правила реагирования**.

c. Нажмите на кнопку **Добавить**.

d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

e. В дереве шагов выберите **Проверка параметров**.

f. Нажмите на кнопку **Сохранить и обновить параметры служб**.

g. Нажмите на кнопку **Сохранить**.

Правило реагирования будет привязано к коррелятору и готово к использованию.

Интеграция с Kaspersky Secure Mail Gateway

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить интеграцию с системой анализа и фильтрации почтового трафика Kaspersky Secure Mail Gateway (далее также "KSMG").

Настройка интеграции заключается в создании правил реагирования KUMA, которые позволяют запускать задачи KSMG. Задачи должны быть предварительно созданы в веб-интерфейсе KSMG.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в KSMG
2. Подготовка скрипта для правила реагирования
3. **Настройка правила реагирования KUMA**

Настройка интеграции в KSMG

Чтобы подготовиться к интеграции в KSMG:

1. Подключитесь к веб-интерфейсу KSMG под учетной записью администратора и создайте роль с правами на просмотр и создание/изменение правила.

   Подробнее о создании роли см. *справку Kaspersky Secure Mail Gateway*.

2. Назначьте созданную роль пользователю с NTML-аутентификацией.

   Вы можете использовать учетную запись локального администратора Administrator.

3. В разделе **Правила** нажмите **Создать**.

4. В левой панели выберите раздел **Общие**.

5. Включите использование правила с помощью переключателя **Статус**.

6. В поле **Название правила** введите название нового правила.

7. В блоке параметров **Режим** выберите один из вариантов обработки сообщений, соответствующий критериям этого правила.

8. В блоке параметров **Отправитель** на вкладке **Адреса эл. почты** укажите несуществующий или заведомо вредоносный адрес отправителя.

9. В блоке параметров **Получатель** на вкладке **Адреса эл. почты** укажите требуемых получателей или символ "*", чтобы выбрать всех получателей.

10. Нажмите на кнопку **Сохранить**.

11. В веб-интерфейсе KSMG откройте только что созданное правило.

12. Запишите значение ID, отображаемое в конце адреса страницы в адресной строке браузера.

    Это значение будет использовано при настройке правила реагирования в KUMA.

Подготовка к интеграции в KSMG будет завершена.

Подготовка скрипта для интеграции с KSMG

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка IP-адреса или адреса электронной почты отправителя сообщения в KSMG:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

   b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

      Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт и библиотеку по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<`ID коррелятора из шага 1`>/scripts/.

4. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 3 при помощи команды:

   ```
   cd /opt/kaspersky/kuma/correlator/< ID коррелятора из шага 1 >/scripts/
   ```

5. Выполните следующую команду:

   ```
   chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py
   ```

Скрипт будет готов к использованию.

Импорт информации об активах из RedCheck

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

RedCheck – это система контроля защищенности и управления информационной безопасностью организации.

Вы можете импортировать в KUMA сведения об активах из отчетов сканирования сетевых устройств, проведенного с помощью RedCheck.

Импорт доступен из простых отчетов "Уязвимости" и "Инвентаризация" в формате CSV, сгруппированных по устройствам.

Импортированные ресурсы отображаются в Консоли OSMP в разделе **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**. При необходимости вы можете редактировать параметры активов.

Импорт данных происходит через API с помощью утилиты redcheck-tool.py. Для работы утилиты требуется Python версии 3.6 или выше и следующие библиотеки:

- csv
- re
- json
- requests
- argparse
- sys

Чтобы импортировать данные об активах из отчета RedCheck:

1. Сформируйте в RedCheck отчет о сканировании сетевых активов в формате CSV и скопируйте файл отчета на сервер со скриптом.

   Подробнее о задачах на сканирование и форматах выходных файлов см. в документации RedCheck.

2. Создайте файл с токеном для доступа к KUMA REST API.

   Учетная запись, для которой создается токен, должна отвечать следующим требованиям:

   - Роль Администратора или Аналитика.
   - Доступ к тенанту, в который будут импортированы активы.
   - Права на использование API-запросов GET /assets, GET /tenants, POST/assets/import.

3. Скачайте скрипт по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

4. Скопируйте утилиту redcheck-tool.py на сервер с Ядром KUMA и сделайте файл утилиты исполняемым при помощи команды:

   ```
   chmod +x <путь до файла redcheck-tool.py>
   ```

5. Запустите утилиту redcheck-tool.py с помощью следующей команды:

   ```
   python3 redcheck-tool.py --kuma-rest <адрес и порт сервера KUMA REST API> --token
   <API-токен> --tenant <название тенанта, куда будут помещены активы> --vuln-report
   <полный путь к файлу отчета "Уязвимости"> --inventory-report <полный путь к файлу
   отчета "Инвентаризация">
   ```

Пример:
```
python3 --kuma-rest example.kuma.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report
/home/user/vuln.csv --inventory-report /home/user/inventory.csv
```

Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения расширенного отчета о полученных активах `-v`. Подробное описание доступных флагов и команд приведено в таблице "Флаги и команды утилиты redcheck-tool.py". Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета RedCheck в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Пример:
```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

Пример расширенной информации об импорте:
```
[inventory import] Host: localhost Code: 200 Response: {'insertedIDs': {'0': '52ca11c6-a0e6-4dfd-8ef9-
bf58189340f8'}, 'updatedCount': 0, 'errors': []}
[inventory import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {'0': '1583e552-5137-4164-92e0-
01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error] Host: localhost Skipped asset with FQDN localhost or IP 127.0.0.1
[software import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.1 Code: 200 Response: {'insertedIDs': {'0': '0628f683-c20c-4107-abf3-
d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import] Host: localhost Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.3 Code: 200 Response: {'insertedIDs': {'0': 'ed01e0a8-dcb0-4609-ab2b-
91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)
```

Поведение утилиты при импорте активов:

- KUMA перезаписывает данные импортированных через API активов и удаляет сведения об их устраненных уязвимостях.
- KUMA пропускает активы с недействительными данными.

Флаги и команды утилиты redcheck-tool.py

Флаги и команды	Обязательное ли поле	Описание
`--kuma-rest < адрес и порт сервера KUMA >`	Да	По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token < токен >`	Да	Значение в параметре должно содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
`--tenant < название тенанта >`	Да	Название тенанта KUMA, в который будут импортированы активы из отчета RedCheck.
`--vuln-report < полный путь к файлу отчета "Уязвимости" >`	Да	Файл отчета "Уязвимости" в формате CSV.

Флаги и команды	Обязательное ли поле	Описание
`--inventory-report < полный путь к файлу отчета "Инвентаризация" >`	Нет	Файл отчета "Инвентаризация" в формате CSV.
`-v`	Нет	Отображение расширенной информации об импорте активов.

Возможные ошибки

Сообщение об ошибке	Описание
Tenant %w not found	Имя тенанта не найдено.
Tenant search error: Unexpected status Code: %d	При поиске тенанта был получен неожиданный код ответа HTTP.
Asset search error: Unexpected status Code: %d	При поиске актива был получен неожиданный код ответа HTTP.
[%w import][error] Host: %w Skipped asset with FQDNlocalhost or IP 127.0.0.1	При импорте информации инвентаризации/уязвимостей было пропущено устройство cfqdn=localhost или ip=127.0.0.1.

Настройка получения событий Sendmail

Вы можете настроить получение событий из почтового агента Sendmail в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования Sendmail.
2. Настройка сервера источника событий.
3. Создание коллектора KUMA.

   Для получения событий Sendmail в мастере установки коллектора используйте следующие значения:

   - На шаге **Парсинг событий** выберите нормализатор **[OOTB] Sendmail syslog**.
   - На шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.
4. Установка коллектора KUMA.
5. Проверка поступления событий Sendmail в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Sendmail выполнена правильно в Консоли OSMP в разделе Поиск связанных событий.

Настройка журналирования Sendmail

По умолчанию события системы Sendmail записываются в syslog.

Чтобы убедиться в правильности настройки журналирования:

1. Подключитесь по SSH к серверу, на котором установлена система Sendmail.
2. Выполните следующую команду:

   ```
   cat /etc/rsyslog.d/50-default.conf
   ```

   Команда должна вернуть следующую строку:

```
mail.* -/var/log/mail.log
```

Если журналирование настроено корректно, вы можете перейти к настройке передачи событий Sendmail.

Настройка передачи событий Sendmail

Для передачи событий от сервера, на котором установлен почтовый агент Sendmail, в коллектор KUMA используется служба rsyslog.

Чтобы настроить передачу событий Sendmail в коллектор:

1. Подключитесь к серверу, на котором установлен Sendmail, под учетной записью с административными привилегиями.

2. В директории /etc/rsyslog.d/ создайте файл Sendmail-to-siem.conf и добавьте в него строку:

   ```
   If $programname contains 'sendmail' then @< <IP-адрес коллектора> : <порт коллектора> >
   ```

   Пример:
   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'sendmail' then @@< <IP-адрес коллектора> : <порт коллектора> >
   ```

3. Создайте резервную копию файла /etc/rsyslog.conf.

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения

6. Перезапустите службу rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Настройка интеграции с внешней SIEM-системой

OSMP может отправлять информацию об алертах и действиях пользователей в веб-интерфейсе приложения во внешнюю SIEM-систему, которая уже используется в вашей организации, по протоколу Syslog.

В качестве внешней SIEM-системы может выступать:

- Kaspersky Unified Monitoring and Analysis Platform (KUMA)

- SIEM-система стороннего производителя

Для передачи данных вам нужно создать точку назначения типа tcp или udp в зависимости от выбранного протокола – TCP или UDP. При передаче данных по протоколу TCP вы можете использовать TLS-шифрование. Для этого при создании точки назначения укажите TLS-сертификат.

Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой:

1. В окне создания точки назначения типа tcp перейдите на вкладку **Дополнительные параметры**.

2. В поле **Режим TLS** выберите одно из значений:

   - **Нестандартный CA**

     Выберите это значение, если хотите загрузить файл сертификата. В поле **Нестандартный CA** укажите секрет, содержащий файл сертификата. Вы можете выбрать существующий секрет или создать секрет. Чтобы создать секрет, вам нужно выбрать в списке значение **Создать** и в открывшемся окне загрузить TLS-сертификат.

   - **Нестандартный PFX**

     Выберите это значение, если хотите загрузить файл сертификата в формате PFX. В поле **PFX секрет** укажите секрет, содержащий файл сертификата. Вы можете выбрать существующий секрет или создать секрет. Чтобы создать секрет, вам нужно выбрать в списке значение **Создать** и в открывшемся окне загрузить PFX-файл, содержащий TLS-сертификат.

3. При необходимости настройте другие параметры точки назначения. Затем нажмите на кнопку **Создать**.

Загруженный TLS-сертификат будет использоваться для шифрования соединения с SIEM-системой.

Управление KUMA

В этом разделе описываются общие параметры KUMA.

Настройка параметров Ядра KUMA

Чтобы настроить параметры Ядра KUMA:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Общее**.

   Откроется окно **Общее**.

3. В блоке **Параметры ядра** укажите значение следующих параметров:

   - С помощью переключателя **Отладка** включите или выключите логирование операций системы (режим отладки). По умолчанию переключатель выключен.

   - Если вы включили режим отладки, с помощью переключателя **Логировать HTTP-KSC запросы** включите или выключите возможность сбросить HTTP-трафик Kaspersky Security Center.

   - Если вы включили возможность сбросить HTTP-трафик Kaspersky Security Center, с помощью переключателя **Периодическое создание дампа** включите или выключите дампы HTTP-запросов и ответов Kaspersky Security Center в журнал событий.

     После включения переключателя **Периодическое создание дампа** в поле **Настройки дампа** укажите параметры дампа.

- В раскрывающемся списке **День начала недели** выберите первый день недели, который будет использоваться во всем экземпляре KUMA. Выбранное значение применяется при выборе периодов и указании временных интервалов во всех разделах KUMA. По умолчанию выбрано значение **Понедельник**. Изменять значение параметра может только пользователь с ролью Главный администратор. Выбранное значение сохраняется в параметрах Ядра KUMA.

- В раскрывающемся списке **Локализация ресурсов KUMA** выберите язык локализации ресурсов KUMA, импортируемых из репозитория. По умолчанию используется английский язык. При изменении параметра только новые ресурсы KUMA будут импортироваться с выбранным языком. Если до этого вы импортировали ресурсы на другом языке, эти ресурсы останутся без изменения. Чтобы поменять язык уже импортированных ресурсов, вам нужно импортировать их из репозитория заново.

  Параметр **Локализация ресурсов KUMA** не зависит от параметра языка интерфейса Kaspersky EDR Expert. Вы можете выбрать разные языки локализации в этих параметрах. В таком случае, например, язык текстов в таблице ресурсов может отличаться от языка локализации интерфейса.

  Параметр **Локализация ресурсов KUMA** не влияет на ресурсы, созданные вручную.

- При необходимости нажмите на кнопку **Перевыпустить**, чтобы перевыпустить сертификат AI-сервиса и внутренний CA-сертификат.

  > После перевыпуска сертификата AI-сервиса необходимо вручную перезапустить все сервисы. Для применения нового сертификата AI-сервиса требуется перезапуск ядра KUMA.

4. Если вы не хотите использовать самоподписанный сертификат KUMA, в блоке **Внешняя TLS-пара** загрузите сертификат и ключ для TLS-пары.

   Нажав на кнопку **Обновить сертификат**, вы можете обновить сертификат для TLS-пары.

5. В блоке **Свойства ядра** укажите значение следующих параметров:

   - Установите флажок **Компактизация SQLite** и укажите нужный объем дискового пространства в ГБ. Это позволяет уменьшить размер базы данных для более эффективного использования дискового пространства.

     По умолчанию флажок установлен, объем дискового пространства – 10 000 ГБ.

   - В поле **Тег активации** укажите применимый тег.

   - В поле **Срок хранения алертов, дни** укажите период хранения алертов в днях. Вы можете указать любое значение больше 0.

     По умолчанию срок хранения составляет 365 дней.

   - В поле **Размер пакетного слияния активов** укажите количество активов в одной группе (пакете), на которые делится общий набор активов перед началом слияния. Каждая группа активов последовательно обрабатывается приложением: активы объединяются, проверяются и сохраняются. Если указано значение 10, то 100 активов будут разделены на 10 групп по 10 активов и каждая группа будет обрабатываться поочередно. Уменьшение значения параметра приводит к формированию более мелких групп, что ускоряет выполнение слияния, так как приложение работает с меньшим объемом данных за один шаг.

     Вы можете указать любое число больше 0. По умолчанию установлено значение 10.

   - В поле **Максимальное число одновременно запускаемых сервисов** укажите количество сервисов, которые KUMA может запускать одновременно.

     По умолчанию установлено значение 10.

Слишком большое количество одновременно запускаемых сервисов может привести к замедлению обработки данных KUMA.

- В поле **Срок действия исключения для создания алерта, часы** укажите период хранения исключений для корреляционных правил в часах. Вы можете указать значение от 1 до 24*365 включительно.

  По умолчанию установлено значение 72 часа.

- В поле **Размер дискового буфера служебной точки назначения (для отправки событий) Core, Мб** укажите размер дискового буфера на ядре, который выделяется под каждый сервис. Буфер используется, когда внутренние события не удалось отправить на корреляторы. Вы можете установить любой размер буфера больше 0.

  По умолчанию установлено значение 1024 MB.

- В поле **Таймаут отправки событий через служебную точку назначения Core, секунды** укажите время ожидания установки соединения с сервисом при отправке событий. Вы можете указать любое время ожидания больше 0 секунд.

  По умолчанию установлено значение 15 секунд.

- В поле **Час суток, в который Core имеет право выполнять задачи по самообслуживанию** укажите время (в формате UTC), когда ядро может осуществлять операции по самостоятельному обслуживанию. Ядро KUMA выполняет такие операции ежедневно. Вы можете указать значение от 0 до 23 включительно.

  Рекомендуется проводить операции по обслуживанию Ядра KUMA в ночное время, когда пользователи не используют функциональные возможности Ядра KUMA.

  По умолчанию установлено значение 1 (время в формате UTC).

- В поле **Максимальный размер хранимого файла, Мб** укажите максимальный размер сжатых данных загружаемой базы GeoIP и пакетов репозитория.

  По умолчанию указано значение 300 МБ.

- В поле **Срок хранения истории ресурсов, дни** укажите время хранения истории изменения ресурсов в днях. Вы можете установить любое значение больше или равное 0.

  По умолчанию указано значение 12 дней.

- В поле **Время ожидания запроса кластеров из UI, секунды** укажите время, в течение которого веб-клиент KUMA ждет ответ на запрос списка хранилищ. Вы можете установить любое значение больше 0.

  По умолчанию указано значение 30 секунд.

- В поле **Время ожидания проверки работоспособности узлов хранилища, секунды** укажите время ожидания ответа на запрос о проверке доступности определенных узлов хранилища. Вы можете установить любое значение больше 0.

  По умолчанию указано значение 30 секунд.

- При необходимости в поле **Имя хоста и порт балансировщика KUMA UI** укажите имя хоста и порт балансировщика пользовательского интерфейса KUMA.

  Учитывая распределенный характер ядра KUMA, можно развернуть несколько элементов ядра, которые будут работать как кластер. Вы можете настроить параметры обращения кластера через балансировщик.

Вы можете указать только один URL балансировщика.

URL балансировщика указывается в формате `hostname:port`, где:

- `hostname` – имя устройства балансировщика;
- `port` – порт балансировщика.

Другие форматы ввода URL балансировщика не допускаются.

6. Нажмите **Сохранить**.

Прокси-серверы

Прокси-серверы используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http.

Доступные параметры:

- **Название** (обязательно) – уникальное имя прокси-сервера. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Секрет отдельно** – если этот флажок установлен, в окне отображается обязательное поле **URL**, в котором можно указать URL подключения, и раскрывающийся список **Секрет** с секретами типа "credentials". Таким образом вы сможете просматривать информацию о подключении без необходимости повторно создавать большое количество подключений, если изменился пароль учетной записи, которую вы использовали для подключений. Если флажок снят, поля **URL** и **Секрет** недоступны. По умолчанию флажок снят.
- **URL** (обязательное) – поле для указания URL подключения. URL используется вместе с секретом типа "credentials". Поле доступно, если установлен флажок **Секрет отдельно**.
- **Секрет** – раскрывающийся список для выбора существующего секрета или создания секрета типа "credentials". Раскрывающийся список доступен, когда установлен флажок **Секрет отдельно**.
- **Брать URL из секрета** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранятся URL прокси-серверов. При необходимости секрет можно указать в окне создания прокси-сервера с помощью значка плюса (+). Выбранный секрет можно изменить, нажав на значок карандаша ( ).
- **Не использовать на доменах** – один или несколько доменов, к которым требуется прямой доступ.
- **Описание** – вы можете добавить до 4000 символов Юникода.

Подключение к SMTP-серверу

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Пользователи будут получать уведомления, если в параметрах их профиля установлен флажок **Получать уведомления по почте**.

Для обработки уведомлений KUMA можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в Консоли OSMP в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общие** → **Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.
2. Откроется окно с параметрами KUMA.
3. В блоке **Другое** нажмите **Общие**.
4. Откроется окно **Общее**.
5. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:
   - **Выключено** – установите этот флажок, если хотите отключить подключение к SMTP-серверу.
   - **Адрес сервера** (обязательно) – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
   - **Порт** (обязательно) – порт подключения к почтовому серверу. Значение должно быть целым числом от 1 до 65 535.
   - **От кого** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.
   - **Псевдоним сервера Ядра KUMA** – название сервера Ядра KUMA, которое используется в вашей сети. Должно отличаться от полного доменного имени (FQDN).
   - При необходимости в раскрывающемся списке **Секрет** выберите секрет типа **credentials**, в котором записаны учетные данные для подключения к SMTP-серверу.

     Добавить секрет

     Чтобы создать секрет:

     1. В поле **Название** введите название секрета.
     2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.
     3. При необходимости в поле **Описание** введите описание секрета.
     4. Нажмите на кнопку **Создать**.

     Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.

- Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.

  Уведомления о срабатывании политики мониторинга от источника будут повторяться через выбранный период, пока статус источника не станет вновь зеленым.

  Если вы выберете значение **Не повторять**, уведомление о срабатывании политики мониторинга придет только один раз.

- Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

- Нажмите на кнопку **Проверить подключение**. KUMA отправит тестовое сообщение на адрес электронной почты, указанный в профиле текущего пользователя. Тестовое сообщение будет отправлено, даже если в профиле пользователя не установлен флажок **Получать уведомления по почте**.

  Проверьте ваш почтовый ящик. Если тестовое сообщение доставлено, SMTP-сервер настроен корректно. Если при отправке сообщения возникает ошибка, проверьте параметры SMTP-сервера. Ошибка отображается в интерфейсе, а также записывается в журнал Ядра KUMA. Если сообщение отправлено, но не доставлено в почтовый ящик, проверьте журнал SMTP-сервера на наличие сообщений об ошибках.

  Мы рекомендуем отправлять тестовое сообщение при каждом изменении параметров SMTP-сервера или шаблона уведомлений.

6. Нажмите на кнопку **Сохранить**.

Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты от KUMA.

Работа с задачами Kaspersky Security Center

Вы можете подключить активы Kaspersky Security Center к KUMA и загружать на эти активы обновления баз и модулей приложений или запускать на них антивирусную проверку с помощью задач Kaspersky Security Center. Задачи запускаются в Консоли KUMA.

Для запуска задач Kaspersky Security Center на активах, подключенных к KUMA, рекомендуется использовать следующий сценарий:

1. **Создание в Консоли администрирования Kaspersky Security Center учетной записи пользователя**

   Данные этой учетной записи используются при создании секрета для установки соединения с Kaspersky Security Center и могут использоваться при создании задачи.

   Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. **О создании задач KUMA в Kaspersky Security Center**

3. **Настройка интеграции KUMA с Kaspersky Security Center**

4. **Импорт информации об активах Kaspersky Security Center в KUMA**

5. **Назначение категории импортированным активам**

   После импорта активы автоматически помещаются в группу **Устройства без категории**. Вы можете назначить импортированным активам одну из существующих категорий или создать категорию и назначить ее активам.

6 **Запуск задач на активах**

Вы можете запускать задачи вручную в информации об активе или настроить автоматический запуск задач.

О создании задач KUMA в Kaspersky Security Center

Вы можете запустить на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей программы и задачу антивирусной проверки. На активах должны быть установлены приложения Kaspersky Endpoint Security for Windows или Kaspersky Endpoint Security for Linux. Задачи создаются в Консоли OSMP.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security for Windows см. в справке *Kaspersky Endpoint Security for Windows*.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security for Linux см. в справке *Kaspersky Endpoint Security for Linux*.

Имя задач должно начинаться с "kuma" (без учета регистра и без кавычек). Например, `KUMA antivirus check`. В противном случае задача не отображается в списке доступных задач в Консоли KUMA.

Запуск задач Kaspersky Security Center вручную

Вы можете вручную запускать на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей программы и задачу антивирусной проверки. На активах должны быть установлены приложения Kaspersky Endpoint Security for Windows или Kaspersky Endpoint Security for Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Чтобы запустить задачу Kaspersky Security Center вручную:

1. В Консоли KUMA перейдите в раздел **Активы** и выберите актив, импортированный из Kaspersky Security Center.

   Откроется окно **Информация об активе**.

2. Нажмите на **Реагирование OSMP**.

Кнопка отображается, если подключение к Kaspersky Security Center, к которому принадлежит выбранный актив, включено.

3. В открывшемся окне **Выберите задачу** установите флажки рядом с задачами, которые вы хотите запустить, и нажмите на кнопку **Запустить**.

Kaspersky Security Center запускает выбранные задачи.

Некоторые типы задач доступны только для определенных активов.

Информация об уязвимостях и программном обеспечении доступна только для активов с операционной системой Windows.

Автоматический запуск задач Kaspersky Security Center

Вы можете настроить автоматический запуск задачи обновления антивирусных баз и модулей программы и задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA. На активах должны быть установлены приложения Kaspersky Endpoint Security for Windows или Kaspersky Endpoint Security for Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Настройка автоматического запуска задач Kaspersky Security Center включает следующие этапы:

Шаг 1. Добавление правила корреляции

Чтобы добавить правило корреляции:

1. В Консоли KUMA выберите раздел **Ресурсы**.

2. Выберите **Правила корреляции** и нажмите на кнопку **Добавить правило корреляции**.

3. На вкладке **Общие** укажите следующие параметры:

   a. В поле **Название** укажите название правила.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   c. В раскрывающемся списке **Тип** выберите **simple**.

   d. В поле **Наследуемые поля** добавьте следующие поля: DestinationAssetID.

e. При необходимости укажите значения для следующих полей:

- В поле **Частота срабатываний** укажите максимальное количество срабатываний правила в секунду.
- В поле **Уровень важности** укажите уровень важности алертов и корреляционных событий, которые будут созданы в результате срабатывания правила.
- В поле **Описание** укажите любую дополнительную информацию.

4. На вкладке **Селекторы** → **Параметры** выполните следующие действия:

a. В раскрывающемся списке **Фильтр** выберите **Создать**.

b. В поле **Условия** нажмите на кнопку **Добавить группу**.

c. В поле с оператором для добавленной группы выберите **И**.

d. Добавьте условие для фильтрации по значению поля DeviceProduct:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите поле события.
4. В поле **Поле события** выберите DeviceProduct.
5. В поле **Оператор** выберите =.
6. В поле **Правый операнд** выберите **константа**.
7. В поле **Значение** введите `OSMP`.

e. Добавьте условие для фильтрации по значению поля Name:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите поле события.
4. В поле события выберите Name.
5. В поле **Оператор** выберите =.
6. В поле **Правый операнд** выберите **константа**.
7. В поле **значение** введите название события. При возникновении этого события задача запускается автоматически.

   Например, если вы хотите, чтобы задача *Антивирусная проверка* запускалась при регистрации событий Kaspersky Security Center *Обнаружен вредоносный объект*, вам нужно указать в поле **значение** это имя.

   Имя события можно посмотреть в поле **Name** в информации о событии.

5. На вкладке **Действия** укажите следующие параметры:

   a. В разделе **Действия** откройте раскрывающийся список **На каждом событии**.

   b. Установите флажок **Отправить на дальнейшую обработку**.

      Другие поля заполнять не требуется.

6. Нажмите на кнопку **Сохранить**.

Правило корреляции будет создано.

Шаг 2. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

> В поле DeviceHostName должно отображаться доменное имя (FQDN) актива. Если оно не отображается, вам нужно создать запись для этого актива в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

Шаг 3. Добавление фильтра

Чтобы добавить фильтр:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Фильтры** и нажмите на кнопку **Добавить фильтр**.
3. В поле **Название** укажите название фильтра.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В поле **Условия** нажмите на кнопку **Добавить группу**.
6. В поле с оператором для добавленной группы выберите **И**.
7. Добавьте условие для фильтрации по значению поля DeviceProduct:

   a. В поле **Условия** нажмите на кнопку **Добавить условие**.

   b. В поле с условием выберите **Если**.

   c. В поле **Левый операнд** выберите поле события.

   d. В поле **Поле события** выберите Type.

   e. В поле **Оператор** выберите =.

   f. В поле **Правый операнд** выберите **константа**.

   g. В поле **значение** введите 3.

8. Добавьте условие для фильтрации по значению поля Name:

   a. В поле **Условия** нажмите на кнопку **Добавить условие**.

   b. В поле с условием выберите **Если**.

   c. В поле **Левый операнд** выберите поле события.

   d. В поле события выберите Name.

   e. В поле **Оператор** выберите =.

   f. В поле **Правый операнд** выберите **константа**.

   g. В поле **значение** введите имя правила корреляции, созданного на шаге 1.

Шаг 4. Добавление правила реагирования

Чтобы добавить правило реагирования:

1. В Консоли KUMA выберите раздел **Ресурсы**.

2. Выберите **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.

3. В поле **Название** укажите название правила.

4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

5. В раскрывающемся списке **Тип** выберите **Реагирование через OSMP**.

6. В раскрывающемся списке **Задача Open Single Management Platform** выберите задачу Kaspersky Security Center, которую требуется запустить.

7. В раскрывающемся списке **Поле события** выберите DestinationAssetID.

8. В поле **Рабочие процессы** укажите количество процессов, которые служба может запускать одновременно.

   По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлена служба коррелятора.

- В поле **Описание** вы можете добавить до 4000 символов Юникода.
- В раскрывающемся списке **Фильтр** выберите фильтр, добавленный на шаге 3 этой инструкции.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если правила реагирования принадлежат общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от Сервера Kaspersky Security Center, к которому подключен главный тенант.

Если в правиле реагирования выбрана задача, которая отсутствует на Сервере администрирования Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Шаг 5. Добавление правила реагирования в коррелятор

Чтобы добавить правило реагирования в коррелятор:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Корреляторы**.
3. В списке корреляторов выберите коррелятор, добавленный на шаге 2 этой инструкции.
4. В дереве шагов выберите **Правила реагирования**.
5. Нажмите на кнопку **Добавить**.
6. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 4 этой инструкции.
7. В дереве шагов выберите **Проверка параметров**.
8. Нажмите на кнопку **Сохранить и перезапустить службы**.
9. Нажмите на кнопку **Сохранить**.

   Правило реагирования будет добавлено в коррелятор.

Автоматический запуск задачи обновления антивирусных баз и модулей приложения или задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA, будет настроен. Задачи запускаются при обнаружении угрозы на активах и получении KUMA соответствующих событий.

Проверка статуса задач Kaspersky Security Center

В Консоли KUMA можно проверить, была ли запущена задача Kaspersky Security Center или завершен ли поиск событий из коллектора, который прослушивает события Kaspersky Security Center.

Чтобы выполнить проверку статуса задач Kaspersky Security Center:

1. Выберите раздел KUMA **Ресурсы** → **Активные сервисы**.

2. Выберите коллектор, настроенный на получение событий с Сервера администрирования Kaspersky Security Center, и нажмите на кнопку **Перейти к событиям**.

   Откроется новая вкладка браузера в разделе **События** KUMA. В таблице отобразятся события с Сервера администрирования Kaspersky Security Center. Статус задач отображается в столбце **Название**.

Поля событий Kaspersky Security Center:

- **Name** (Название) – статус или тип задачи.

- **Message** (Сообщение) – сообщение о задаче или событии.

- **FlexString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, полученного от Kaspersky Security Center. Например, `FlexString1Label=TaskName`.

- **FlexString<номер>** (Настраиваемое поле <номер>) – значение атрибута, указанного в поле поля FlexString<номер>Label. Например, `FlexString1=Download updates`.

- **DeviceCustomNumber<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к состоянию задачи. Например, `DeviceCustomNumber1Label=TaskOldState`.

- **DeviceCustomNumber<номер>** (Настраиваемое поле <номер>) – значение, относящееся к состоянию задачи. Например, `DeviceCustomNumber1=1` означает, что задача выполняется.

- **DeviceCustomString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к обнаруженной уязвимости: например, название вируса, уязвимого приложения.

- **DeviceCustomString<номер>** (Настраиваемое поле <номер>) – значение, относящееся к обнаруженной уязвимости. Например, пары атрибут-значение `DeviceCustomString1Label=VirusName` и `DeviceCustomString1=EICAR-Test-File` означают, что обнаружен тестовый вирус EICAR.

Журналы KUMA

Журналы компонентов.

По умолчанию для всех компонентов KUMA в журнале регистрируются только ошибки. Чтобы получать детализированные данные в журналах, следует настроить в параметрах компонента режим **Отладка**.

Журнал пополняется, пока не достигнет размера 5 ГБ. По достижении 5 ГБ журнал архивируется и события начинают записываться в новый журнал. Архивы хранятся в папке с журналами в течение 7 дней, по истечении 7 дней архив удаляется. Одновременно на сервере хранится не более четырех заархивированных журналов. При появлении нового архива журнала, если архивов становится больше четырех, самый давний архив удаляется.

Режим **Отладка** доступен для следующих компонентов:

Службы:
 	
• Хранилище
• Корреляторы
• Коллекторы
• Агенты
	Как включить: в параметрах службы с помощью переключателя **Отладка**.
	
	Где хранятся: в директории установки службы. Например, /opt/kaspersky/kuma/<имя службы>/log/<имя службы>. Журналы событий сервисов можно скачать в Консоли KUMA в разделе **Ресурсы** → **Активные сервисы**, выбрав нужный сервис и нажав на кнопку **Журнал событий**.
	
	Журналы на машинах Linux можно просмотреть с помощью команды journalctl и tail. Например:
	
	• Хранилище. Чтобы вернуть последние журналы из хранилища, установленного на сервере, выполните команду:
	`journalctl -f -u kuma-storage-< идентификатор хранилища >`
	
	• Корреляторы. Чтобы вернуть последние журналы из корреляторов, установленных на сервере, выполните команду:
	`journalctl -f -u kuma-correlator-< идентификатор коррелятора >`
	
	• Коллекторы. Чтобы вернуть последние журналы определенного коллектора, установленного на сервере, выполните команду:
	`journalctl -f -u kuma-collector-< идентификатор коллектора >`
	
	• Агенты. Чтобы вернуть последние журналы агента, установленного на сервере, выполните команду:
	`tail -f /opt/kaspersky/agent/< идентификатор агента >/log/agent`
	Активность агентов на устройствах под управлением Windows всегда регистрируется, если им назначено разрешение на вход в систему в качестве службы. Данные указываются более подробно, если установлен флажок **Отладка**. Журналы агентов на машинах Windows можно просмотреть в файле %PROGRAMDATA%\Kaspersky Lab\KUMA\<идентификатор агента>\agent.log. Журналы агентов на машинах Linux хранятся в директории установки агента.

Ресурсы: • Коннекторы • Точки назначения • Правила обогащения	Как включить: в параметрах службы, к которому привязан ресурс, с помощью переключателя **Отладка**. Где хранятся: журналы хранятся на машине, на которой установлена служба, использующая требуемый ресурс. Детализированные данные для ресурсов можно посмотреть в журнале службы, к которой привязан ресурс.

Уведомления KUMA

Стандартные уведомления

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для этого необходимо настроить подключение к SMTP-серверу, а также установить флажок **Получать уведомления по почте** для пользователей, которым должны приходить уведомления.

KUMA автоматически уведомляет пользователей о следующих событиях:

- Создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета).
- Выполнена задача (уведомление получают пользователи, создавшие задачу).
- Доступны новые пакеты с ресурсами. Их можно получить путем обновления хранилища KUMA (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи).

Изменение профиля пользователя KUMA

Чтобы изменить профиль пользователя KUMA:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Доступ** нажмите **Профиль**.

   Откроется окно **Профиль**.

3. Задайте следующие параметры:

   - В поле **Часовой пояс** выберите часовой пояс, в котором должны отображаться временные отметки в KUMA. Список формируется на основе параметров операционной системы пользователя с учетом перехода на летнее время. По умолчанию используется часовой пояс браузера пользователя.
   - Установите флажок **Использовать формат ISO 8601**, чтобы отображать метки времени в формате ISO 8601 (например, 2026-02-08T17:35:27+03:00). Формат применяется в тех разделах веб-интерфейса KUMA, где используется сокращенное или полное отображение даты и времени, и действует во всей Консоли KUMA. Выбранный формат сохраняется в настройках Ядра KUMA.
   - **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от KUMA.
   - **Отображать непечатаемые символы** – установите этот флажок, если хотите, чтобы в веб-интерфейсе KUMA отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку. Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и отключать с помощью комбинации клавиш **`Ctrl/Command+*`**.

     Пробелы и знаки табуляции отображаются во всех полях ввода, кроме **Описание**, в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов, а также в SQL-запросах на поиск событий в разделе **События**. Пробелы отображаются в виде точек. Знак табуляции отображается в виде тире в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов. В других полях знак табуляции отображается в виде одной или двух точек.

     Символ переноса на новую строку отображается во всех полях ввода, поддерживающих многострочный ввод, например, в строке поиска событий.
   - В раскрывающемся списке **Наборы пространств** выберите один или несколько наборов пространств, к которым вы хотите предоставить доступ, установив рядом флажок. Если у пользователя нет выбранных наборов пространств, будет предоставлен доступ к набору пространств по умолчанию.

4. Нажмите на кнопку **Сохранить**.

Профиль пользователя KUMA изменен.

Работа с тенантами

Тенанты отображаются в таблице, размещенной в разделе Настройки → KUMA → Открыть параметры KUMA → Тенанты. Нажимая на столбцы, таблицу можно отсортировать.

Доступные столбцы:

- **Название** – название тенанта.
- **Ограничение EPS** – размер квоты EPS (частота обработки событий в секунду), выделенной тенанту из доступного количества EPS, которое определяется лицензией.
- **Описание** – описание тенанта.
- **Создан** – дата создания тенанта.
- **Последнее обновление** – дата и время изменения информации о тенанте.

Вы можете экспортировать список тенантов, чтобы, например, отображать имена тенантов в виджетах Активные списки или Контекстные таблицы. Для этого экспортируйте список тенантов, чтобы затем импортировать его в словарь. Для этого нажмите на кнопку **Экспортировать** → **Для словаря**. Файл со списком тенантов загружен на ваше устройство.

Также вы можете экспортировать всю информацию из таблицы тенантов в файл. Для этого нажмите на кнопку **Экспорт** → **Все поля**. Файл со списком тенантов загружен на ваше устройство.

Управление сертификатами

В этом разделе описана работа с сертификатами.

Скачивание сертификатов

В веб-интерфейсе OSMP вы можете скачать следующие сертификаты:

- CA-сертификат REST API.

  Сертификат требуется для проверки подлинности API-сервера, обслуживающего публичное API KUMA. Также вы можете использовать этот сертификат при импорте данных из отчетов MaxPatrol.

  Сертификат можно изменить, если вы хотите использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-интерфейса.

  После загрузки сертификат можно импортировать в хранилище доверенных сертификатов операционной системы или браузера. После этого клиент будет доверять TLS-сертификату, который был выпущен OSMP и подписан удостоверяющим центром.

  Скачанный CA-сертификат не предназначен для редактирования. Если необходимо изменить список имен узлов (SAN) или использовать сертификат корпоративного удостоверяющего центра, следует выпустить новый TLS-сертификат и загрузить его в OSMP в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общие** → **Внешняя TLS-пара**.

Если кластер содержит несколько узлов с сервисом Ядра KUMA и предполагается прямое подключение к каждому узлу, рекомендуется использовать TLS-сертификат, в SAN которого указаны FQDN всех узлов с сервисом Ядра KUMA. В противном случае браузер может отображать предупреждение о несоответствии имени узла сертификату.

Указание FQDN узлов в поле Subject Alternative Names (SAN) выполняется на этапе выпуска нового TLS-сертификата. Изменять скачанный CA-сертификат REST API не требуется.

- CA-сертификат Microservice.

  Сертификат требуется для проверки подлинности при подключении источников журналов к пассивным коллекторам с использованием TLS, но без указания собственного сертификата.

- Сертификат AI-сервиса.

  Этот сертификат требуется для установки сервиса **AI-рейтинг и AI-статус активов**.

Чтобы скачать сертификат:

1. В веб-интерфейсе OSMP перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. На панели инструментов в меню (⋮) выберите нужную опцию:
   - **Скачать REST API CA-сертификат**.
   - **Скачать Microservice CA-сертификат**.
   - **Скачать сертификат AI-сервиса**.

Сертификат будет сохранен в папку, указанную в параметрах вашего браузера.

Чтобы скопировать отпечаток сертификата:

1. В веб-интерфейсе OSMP перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. На панели инструментов в меню (⋮) выберите **Копировать отпечаток сертификата**.

Идентификатор отпечатка сертификата скопирован в буфер обмена. Используйте идентификатор отпечатка CA-сертификата в качестве значения параметра `--pair.fingerprint` в команде установки сервиса для проверки подлинности сертификата Ядра KUMA при первом подключении сервиса к Ядру KUMA.

Изменение самоподписанного сертификата веб-интерфейса

Вы можете использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-интерфейса. Например, если вы хотите заменить сертификат веб-интерфейса с самоподписанного CA Core на сертификат, выпущенный корпоративным CA, необходимо предоставить `external.cert` и незашифрованный `external.key` в формате PEM.

В приведенной инструкции описано, как заменить самоподписанный CA Core с помощью корпоративного сертификата в формате PFX. Вы можете использовать инструкцию в качестве примера и адаптировать шаги в соответствии со своими потребностями.

Чтобы заменить сертификат веб-интерфейса OSMP на корпоративный сертификат в формате PFX:

1. Если вы используете сертификат и ключ в PFX-контейнере, в OpenSSL конвертируйте файл PFX в сертификат и зашифрованный ключ в формате PEM:

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nokeys -out external.cert
   ```

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nocerts -nodes -out external.key
   ```

   При выполнении команды потребуется указать пароль от ключа PFX (Enter Import Password).

   Вы получите сертификат `external.cert` и ключ `external.key` в формате PEM.

2. Если вы используете незашифрованный ключ `external.key`, убедитесь, что формат ключа – PKCS#8. Если файл ключа начинается с тега `BEGIN RSA PRIVATE KEY`, OSMP не сможет обработать файл ключа. В этом случае конвертируйте файл с помощью команды:

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   После выполнения команды файл будет начинаться с тега `BEGIN PRIVATE KEY` и OSMP обработает файл ключа.

3. В веб-интерфейсе OSMP откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее**.

4. В блоке параметров **Внешняя TLS-пара** загрузите `external.cert` и незашифрованный `external.key` в формате PEM.

5. Перезапустите Ядро KUMA:

   ```
   systemctl restart kuma-core
   ```

6. Обновите страницу или перезапустите браузер, с помощью которого вы работаете в веб-интерфейсе OSMP.

Сертификат и ключ вашей компании заменены.

Перевыпуск внутренних CA-сертификатов

Перевыпускать внутренний CA-сертификат могут только пользователи с ролью Главный администратор.

Чтобы перевыпустить и применить внутренний CA-сертификат:

1. В веб-интерфейсе откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее**.

2. В блоке Параметры Ядра нажмите на кнопку **Перевыпустить внутренние CA-сертификаты**.

3. В открывшемся окне подтвердите перевыпуск сертификатов.

   CA-сертификаты для сервисов KUMA и CA-сертификат для ClickHouse будут перевыпущены. Перевыпущенные сертификаты требуется применить.

4. Подключитесь к хостам, на которых развернуты сервисы коллектора и коррелятора:

   a. Остановите все сервисы, выполнив команду:

   ```
   sudo systemctl stop kuma-<collector/correlator/metrics>-<service_ID>.service
   ```

   где:

   <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса OSMP.

   b. Удалите файлы `internal.cert` и `internal.key` из директорий `/opt/kaspersky/kuma/<тип сервиса>/<ID сервиса>/certificates`, выполнив следующие команды:

   ```
   sudo rm -f /opt/kaspersky/kuma/<collector/correlator/metrics>/<service_ID>/certificates/internal.cert
   ```

   ```
   sudo rm -f /opt/kaspersky/kuma/<collector/correlator/metrics>/<service_ID>/certificates/internal.key
   ```

5. Подключитесь к хостам, на которых развернуты сервисы хранилища:

   a. Остановите все сервисы хранилища:

   ```
   sudo systemctl stop kuma-<storage>-<service_ID>.service
   ```

   b. Удалите файлы `internal.cert` и `internal.key` из директорий `/opt/kaspersky/kuma/storage/<ID сервиса>/certificates`, выполнив следующие команды:

   ```
   sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.cert
   ```

   ```
   sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.key
   ```

6. Удалите все сертификаты ClickHouse из директории `/opt/kaspersky/kuma/clickhouse/certificates`, выполнив следующие команды:

   ```
   sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
   ```

   ```
   sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
   ```

7. Подключитесь к хостам, на которых развернуты сервисы агентов:

   a. Остановите сервисы агентов Windows и агентов Linux.

   b. Удалите файлы `internal.cert` и `internal.key` из рабочих директорий агентов.

8. Перезапустите Ядро KUMA, чтобы применить новые CA-сертификаты:

   - Для развертывания на одном сервере и распределенного развертывания выполните команду:

   ```
   sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
   ```

- Для развертывания в кластере Kubernetes, на любом контроллере выполните следующие команды:

```
sudo k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
```

```
sudo k0s kubectl rollout restart deployment metrics -n kuma
```

```
sudo k0s kubectl rollout restart deployment/core-deployment -n kuma
```

Рекомендуется перезапускать Ядро KUMA с помощью команды, поскольку перезапуск через веб-интерфейс влияет на перезапуск только контейнера Ядра KUMA, а не весь под целиком.

9. Перезапустите все остановленные сервисы:

```
sudo systemctl start kuma-<collector/correlator/storage/metrics>-<service_ID>.service --pair.fingerprint
<CA_cert_ID>
```

где:

- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса KUMA.
- <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Параметр `--pair.fingerprint` является необязательным. При создании сервиса KUMA автоматически добавляет этот параметр в команду установки и указывает идентификатор отпечатка. Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае KUMA использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра KUMA при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

  Для обеспечения проверки подлинности CA-сертификата Ядра KUMA рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. В этом случае при перевыпуске CA-сертификата необходимо скопировать идентификатор отпечатка в разделе **Ресурсы и сервисы** → **Активные сервисы** → меню (⋮) → **Копировать отпечаток сертификата**.

Внутренние CA-сертификаты будут применены.

Перевыпуск сертификата для отдельного сервиса

Чтобы сбросить сертификат для отдельного сервиса:

1. В веб-интерфейсе откройте раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с тем сервисом, сертификат которого вы хотите перевыпустить.

3. В панели инструментов или в меню ⋮ выберите **Сбросить сертификат**.

> Этот вариант недопустимо использовать для обновления сертификата Ядра KUMA. Чтобы обновить сертификаты Ядра KUMA, их требуется перевыпустить и применить внутренний CA-сертификат.

4. Удалите прежний сертификат в директории установки сервиса.

Решение автоматически сгенерирует новый сертификат. Для работающих сервисов перезапуск не требуется, новый сертификат будет применен автоматически. Если сервис был остановлен, необходимо перезапустить сервис, чтобы применить новый сертификат.

Особенности удаления сертификатов для агентов Windows:

- Если агент находится в зеленом статусе, OSMP удаляет действующий сертификат и создает новый. Агент продолжит работу с новым сертификатом.
- Если агент находится в красном статусе, отображается ошибка, что агент не запущен. В папке установки агента `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<ID агента>\certificates` следует удалить файлы `internal.cert` и `internal.key` и вручную запустить агент. При запуске агента новый сертификат будет создан автоматически.

Особенности удаления сертификатов для агентов Linux:

- Независимо от статуса агента сертификат сбрасывается через веб-интерфейс.
- В папке установки агента `/opt/kaspersky/agent/<ID агента>/certificates` нужно удалить файлы `internal.cert` и `internal.key`.
- Поскольку при сбросе сертификата работа агента будет остановлена, для продолжения работы нужно вручную запустить агент. При запуске агента новый сертификат создается автоматически.

Работа с геоданными

В KUMA можно загрузить список соответствий IP-адресов или диапазонов IP-адресов географическим данным, чтобы затем использовать эту информацию при обогащении событий.

Формат геоданных

Геоданные можно загрузить в KUMA в виде CSV-файла в кодировке UTF-8. В качестве разделителя используется запятая. В первой строке файла указаны заголовки полей: `Network,Country,Region,City,Latitude,Longitude`.

Имя заголовка поля в CSV	Описание поля	Пример
`Сеть`	IP-адрес в одном из следующих форматов: • IP-адрес; • диапазон IP-адресов; • IP-адрес в формате CIDR. Допускается перемешивание IPv4- и IPv6-адресов. Обязательное поле.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Принятое в вашей организации обозначение страны. Например, ее название или код. Обязательное поле.	• `Russia` • `RU`
`Region`	Принятое в вашей организации обозначение области. Например, ее название или код.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	Принятое в вашей организации обозначение города. Например, ее название или код.	• `Yekaterinburg` • `65701000001`
`Latitude`	Широта описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`56,835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`60,612778`

Конвертация геоданных из MaxMind и IP2Location

В KUMA можно использовать геоданные, полученные из MaxMind, IP2Location, а также совместимые с ними по формату. При этом наименование конвертируемого файла должно удовлетворять шаблону: (GeoIP2|GeoLite2)-(City|Country)-Blocks-IPv(4|6).csv. Однако вам нужно конвертировать файлы, которые вы хотите использовать, в формат, поддерживаемый KUMA. Конвертацию можно произвести с помощью приведенного ниже скрипта. Убедитесь, что файлы не содержат повторяющихся записей. Например, если в файле несколько столбцов, разные записи могут содержать данные из одной сети с одинаковыми геоданными. Такие файлы невозможно конвертировать. Чтобы успешно выполнить конвертацию, убедитесь, что дублирующиеся строки отсутствуют и все строки уникальны по какому-либо полю.

Загрузить скрипт

Для запуска скрипта требуется Python 2.7 или выше.

Команда запуска скрипта:

```
python converter.py --type <тип обрабатываемых геоданных: "maxmind" или "ip2location">
--out <директория, в которую будет помещен CSV-файл с геоданными в формате KUMA> --
input <путь к ZIP-архиву с геоданными из MaxMind или IP2location>
```

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта:
`python converter.py --help`

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out
geoip_maxmind_ru.csv
```

Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла GeoLite2-City-Locations-en.csv из ZIP-архива.

Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out
geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP
IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out geoip_ip2location_ipv4_ipv6.csv
```

Параметр `--lang` для IP2Location не используется.

Обязательные наборы полей

Исходные файлы MaxMind GeoLite2-City-Blocks-IPv4.csv и GeoLite2-City-Blocks-IPv6.csv должны содержать следующий набор полей:

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

Пример набора исходных данных:

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000

1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

Остальные файлы CSV с кодом локали должны содержать следующий набор полей:

geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

Пример набора исходных данных:

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0

7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

Исходные файлы IP2Location должны содержать данные о диапазонах сетей, Country, Region, City, Latitude, Longitude

Пример набора исходных данных:

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"

"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"

"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+0
```

Если исходные файлы будут содержать другой набор полей, отличный от указанного в этом разделе, или каких-то полей будет не хватать, после конвертации отсутствующие поля в итоговом файле CSV будут пустыми.

Импорт и экспорт геоданных

При необходимости в KUMA вы можете вручную импортировать и экспортировать геоданные. Геоданные импортируются и экспортируются в файле формате CSV. При успешном импорте геоданных ранее добавленные данные перезаписываются и в KUMA создается событие аудита.

Чтобы импортировать геоданные в KUMA:

1. Подготовьте CSV-файл с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать в поддерживаемый KUMA формат.

2. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

3. В блоке **Другое** нажмите **Общие**.

   Откроется окно **Общее**.

4. В блоке параметров **Настройка GeoIP** нажмите на кнопку **Импортировать из файла** и выберите CSV-файл с геоданными.

   Дождитесь окончания импорта геоданных. При обновлении страницы загрузка данных прерывается.

Геоданные загружены в KUMA.

Чтобы экспортировать геоданные из KUMA,

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Общие**.

   Откроется окно **Общее**.

3. В блоке параметров **Настройка GeoIP** нажмите на кнопку **Экспортировать**.

Геоданные будут скачаны в виде CSV-файла (в кодировке UTF-8) с названием geoip.csv в соответствии с настройками вашего браузера.

Данные экспортируются в том же формате, в каком они были загружены, за исключением диапазонов IP-адресов. Если в KUMA в импортированном файле диапазон адресов указан в формате `1.0.0.0/24`, то в файле экспорта диапазон отобразится в формате `1.0.0.0-1.0.0.255`.

Сопоставление геоданных по умолчанию

Если при настройке правила обогащения геоданными в качестве источника IP-адреса выбрать поля события `SourceAddress`, `DestinationAddress` и `DeviceAddress`, становится доступна кнопка **Применить сопоставление по умолчанию**. Нажав на эту кнопку, вы можете добавить преднастроенные пары соответствий атрибутов геоданных и полей события (см. таблицы ниже).

Соответствия по умолчанию для поля события SourceAddress

Атрибут геоданных	Поле события
Country	`SourceCountry`
Region	`SourceRegion`
City	`SourceCity`
Latitude	`SourceLatitude`
Longitude	`SourceLongitude`

Соответствия по умолчанию для поля события DestinationAddress

Атрибут геоданных	Поле события
Country	`DestinationCountry`
Region	`DestinationRegion`
City	`DestinationCity`
Latitude	`DestinationLatitude`
Longitude	`DestinationLongitude`

Соответствия по умолчанию для поля события DeviceAddress

Атрибут геоданных	Поле события
Country	`DeviceCountry`
Region	`DeviceRegion`
City	`DeviceCity`
Latitude	`DeviceLatitude`
Longitude	`DeviceLongitude`

Работа с базой знаний

В Консоли OSMP доступен раздел **База знаний**, который позволяет более наглядно организовать работу с пакетами и ресурсами, которые поставляет "Лаборатория Касперского". В этом разделе можно просматривать доступные и установленные пакеты и ресурсы, оценивать покрытие техник MITRE ATT&CK установленными ресурсами, отслеживать актуальность версий ресурсов, выполнять поиск и фильтрацию по заданным параметрам, а также устанавливать отдельные ресурсы или пакеты целиком.

Пакеты содержат наборы ресурсов, предназначенных для настройки OSMP. Пакеты загружаются из репозитория "Лаборатории Касперского".

> Если пакеты из репозитория еще не были загружены, в разделе **База знаний** список пакетов и ресурсов будет пустым. Чтобы получить доступные для установки пакеты и ресурсы, необходимо настроить обновление предустановленных ресурсов.
> Подробнее о настройке получения ресурсов из репозитория см. в разделе Обновление ресурсов.

Чтобы открыть раздел **База знаний**, в Консоли OSMP перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний**.

Раздел содержит виджеты, отображающие сводную информацию о пакетах и ресурсах в вашем экземпляре решения. Чтобы отобразить или скрыть виджеты, нажмите значок . Доступны следующие виджеты:

- **Статус пакетов** – отображает количество пакетов со следующими статусами:
  - **Доступно** – пакет доступен для установки.
  - **Установлено** – пакет установлен целиком.
  - **Экстренно** – пакет содержит ресурсы с высоким приоритетом, которые необходимо установить как можно скорее.
  - **Новое** – пакет был добавлен в репозиторий менее трех месяцев назад и еще не был установлен или просмотрен пользователем.

- **Статус ресурсов** – отображает количество ресурсов различных типов со следующими статусами:
  - **Доступно** – ресурс доступен для установки.
  - **Установлено** – ресурс установлен и не требует обновления.
  - **Требуется обновление** – для ресурса доступна более новая версия в репозитории.
- **Покрыто техниками MITRE, {{ filter }}** – отображает информацию о количестве или проценте техник MITRE ATT&CK, покрытых выбранными ресурсами.

Виджеты также являются фильтрами для таблиц на странице. При выборе значения в виджете таблица автоматически обновляется в соответствии с выбранным фильтром. Например, можно отобразить только ресурсы со статусом **Требуется обновление**.

В разделе отображаются следующие вкладки:

- Пакеты – список пакетов с ресурсами (отображается по умолчанию).
- Ресурсы – список отдельных ресурсов.

Для поиска пакетов или ресурсов используйте поле **Поиск**. Поиск выполняется только на открытой вкладке. При переключении между вкладками введенный поисковый запрос сохраняется и применяется к выбранной вкладке. В поле **Поиск** можно вводить название ресурса, источник событий, тип событий, название пакета или любую подстроку.

Чтобы отфильтровать содержимое вкладок **Пакеты** и **Ресурсы**, нажмите значок фильтра .

Таблицы на вкладках **Пакеты** и **Ресурсы** можно сортировать, нажав на заголовок столбца нужного параметра и выбрав **По возрастанию** или **По убыванию**. Также доступна фильтрация по столбцам **Тип ресурса** или **Статус**, нажав на заголовок необходимого столбца и выбрав значения, которые вы хотите отобразить.

Просмотр сведений о пакете

Чтобы просмотреть доступные пакеты,

в Консоли OSMP откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** и перейдите на вкладку **Пакеты** (отображается по умолчанию).

На вкладке **Пакеты** отображается таблица со списком доступных пакетов, которая содержит следующие столбцы:

- **Название** – название пакета.
- **Версия** – версия пакета.
- **Дата выпуска** – дата выпуска пакета.
- **Типы ресурсов** – типы ресурсов, входящих в состав пакета:
  - Активный лист
  - Контекстная таблица

    - Нормализатор
    - Правило агрегации событий
    - Правило корреляции
    - Правило обогащения
    - Словарь
    - Фильтр
    - Шаблон уведомлений
- **Количество ресурсов** – количество ресурсов в пакете.
- **Статус** – статус пакета:
    - **Доступно** – пакет доступен для установки.
    - **Установлено** – пакет установлен целиком.
    - **Экстренно** – пакет содержит ресурсы с высоким приоритетом, которые необходимо установить как можно скорее.
    - **Новое** – новый пакет, доступный для установки.
- **Описание** – описание пакета.

Чтобы просмотреть информацию о пакете, нажмите на его название. Откроется окно с информацией о пакете, которое содержит вкладки **Общие** и **Журнал изменений**.

На вкладке **Общие** отображается следующая информация:

- название пакета;
- описание;
- дата выпуска;
- версия.

Также эта вкладка содержит блок **Импортируемые ресурсы**, в котором отображается список ресурсов, входящих в состав пакета. В блоке можно отфильтровать ресурсы и выбрать только необходимые для установки.

На вкладке **Журнал изменений** отображается информация об изменениях пакета.

Просмотр сведений о ресурсе

Чтобы просмотреть доступные ресурсы,

в Консоли OSMP откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** и перейдите на вкладку **Ресурсы**.

На вкладке **Ресурсы** отображается таблица со списком доступных ресурсов, которая содержит следующие столбцы:

- **Название** – название ресурса.
- **Тип ресурса** – доступные типы ресурсов:
  - Активный лист
  - Контекстная таблица
  - Нормализатор
  - Правило агрегации событий
  - Правило корреляции
  - Правило обогащения
  - Словарь
  - Фильтр
  - Шаблон уведомлений
- **Дата установки** – дата установки ресурса в KUMA.
- **Тенант** – тенант, в котором установлен ресурс.

  Если один и тот же ресурс установлен в нескольких тенантах, он отображается в таблице как группа. Чтобы просмотреть сведения об установленном ресурсе в каждом тенанте, нужно развернуть группу.
- **Версия** – версия ресурса.
- **Статус** – статус ресурса:
  - **Доступно** – ресурс доступен для установки.
  - **Установлено** – ресурс установлен.
  - **Требуется обновление** – для ресурса доступна новая версия.
- **Названия пакетов** – список пакетов, в которые входит ресурс.
- **Теги производителя** – теги, назначенные производителем ресурса.
- **Техники MITRE** – техники MITRE ATT&CK, связанные с ресурсом.

Чтобы просмотреть информацию о ресурсе, нажмите на его название. Откроется окно с информацией о ресурсе, которое содержит вкладки **Общая информация** и **Связанные ресурсы**.

На вкладке **Связанные ресурсы** вы можете просмотреть ресурсы, связанные с выбранным ресурсом. Вы также можете просмотреть зависимости на вкладке **Ресурсы** по кнопке **Показать зависимости**.

Установка и обновление пакетов и ресурсов

Установка пакета

Пакет получает статус **Установлено** только в том случае, если установлены все ресурсы, входящие в его состав.

Чтобы установить пакет целиком:

1. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** → **Пакеты**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив нужного пакета и нажмите на кнопку **Установить**.
   - Нажмите на название пакета и в открывшемся окне нажмите на кнопку **Установить**.
3. Выберите тенант.
4. Нажмите на кнопку **Установить**.
   После этого ресурсы будут импортированы OSMP и доступны для дальнейшей настройки.

Установка отдельных ресурсов

Чтобы установить отдельные ресурсы из пакета:

1. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** → **Ресурсы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив нужных ресурсов и нажмите на кнопку **Установить**.
   - Нажмите на название ресурса и в открывшемся окне нажмите на кнопку **Установить**.
3. Выберите тенант.
4. Нажмите на кнопку **Установить**.

Обновление ресурсов

Если для установленного ресурса доступна новая версия, ресурс получает статус **Требуется обновление**.

Чтобы обновить ресурс:

1. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** → **Ресурсы**.
2. Установите флажок напротив одного или нескольких ресурсов со статусом **Требуется обновление**.
3. Нажмите на кнопку **Обновить**.

Ресурсы KUMA

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Эти компоненты собираются в различных комбинациях в наборы ресурсов для сервисов, которые затем используются в качестве основы для создания сервисов KUMA.

Ресурсы содержатся в Консоли KUMA в разделе **Ресурсы.**

В блоках **Ресурсы** и **Правила** доступны следующие типы ресурсов:

- **Нормализаторы** – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в KUMA. После обработки в нормализаторе сырое событие становится нормализованным и может обрабатываться другими ресурсами и сервисами KUMA.
- **Коннекторы** – в ресурсах этого типа содержатся параметры для установления сетевых подключений.
- **Точки назначения** – в ресурсах этого типа содержатся параметры для пересылки событий в пункт дальнейшей обработки или хранения.
- **Фильтры** – в ресурсах этого типа содержатся условия для отсева или выделения отдельных событий из потока событий.
- **Активные листы** – ресурсы этого типа используются корреляторами для динамической работы с данными при анализе событий по правилам корреляции.
- **Словари** – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и службам KUMA.
- **Прокси-серверы** – в ресурсах этого типа содержатся параметры использования прокси-серверов.
- **Секреты** – ресурсы этого типа используются для безопасного хранения конфиденциальной информации (например, учетных данных), которые должны использоваться KUMA для взаимодействия с внешними службами.
- **Контекстные таблицы** – ресурсы этого типа используются корреляторами KUMA для анализа событий в соответствии с правилами корреляции.
- **Шаблоны уведомлений** – ресурсы этого типа используются при рассылке уведомлений о новых алертах.
- **Правила корреляции** – в ресурсах этого типа содержатся правила определения в событиях закономерностей, указывающих на угрозы. Если условия, заданные в этих ресурсах, выполняются, создается корреляционное событие.
- **Правила агрегации** – в ресурсах этого типа содержатся правила для объединения нескольких однотипных базовых событий в одно агрегационное событие.

- **Правила обогащения** – в ресурсах этого типа содержатся правила для дополнения событий информацией из сторонних источников.

- **Правила реагирования** – ресурсы этого типа используются в корреляторах для запуска, например, скриптов или задач Kaspersky Security Center при выполнении определенных условий.

- **Правила сбора и анализа данных** – в ресурсах этого типа содержатся правила, которые позволяют планировать выполнение SQL-запросов с агрегационными функциям в хранилище по заданному расписанию. Далее по данным, полученным от SQL-запросов, осуществляется корреляция.

При нажатии на тип ресурса открывается окно, в котором отображается таблица с имеющимися ресурсами этого типа. Таблица содержит следующие столбцы:

- **Название** – имя ресурса. Может использоваться для поиска и сортировки ресурсов.

- **Последнее обновление** – дата и время последнего обновления ресурса. Может использоваться для сортировки ресурсов.

- **Создал** – имя пользователя, создавшего ресурс.

- **Описание** – описание ресурса.

Максимальный размер таблицы не ограничен. Если вы хотите выбрать все ресурсы, прокрутите таблицу до конца и установите флажок **Выбрать все**, таким образом все доступные в таблице ресурсы будут выбраны.

Ресурсы можно расположить по папкам. В левой части окна отображается структура папок: корневые папки соответствуют тенантам и содержат перечень всех ресурсов тенанта. Во всех остальных папках, вложенных в корневую, отображаются ресурсы отдельной папки. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Ресурсы можно создавать, редактировать, копировать, перемещать между папками и удалять. Ресурсы можно также экспортировать и импортировать.

KUMA поставляется с набором предустановленных ресурсов, которые можно узнать по названию `[OOTB] < название_ресурса >`. OOTB-ресурсы защищены от внесения изменений.

Если вы хотите адаптировать предустановленный OOTB-ресурс к инфраструктуре своей организации:

1. В разделе **Ресурсы**-<тип ресурсов> и выберите OOTB-ресурс, который вы хотите изменить.

2. В верхней части Консоли KUMA нажмите на кнопку **Дублировать**, а затем нажмите на кнопку **Сохранить**.

   В веб-интерфейсе появится новый ресурс с названием `[OOTB]< название_ресурса > - copy`.

3. Внесите необходимые изменения в созданную копию предустановленного ресурса и сохраните изменения.

Адаптированный ресурс доступен для использования.

Операции с ресурсами

Вы можете управлять ресурсами KUMA: создавать, перемещать, копировать, редактировать и удалять ресурсы, а также импортировать и экспортировать их. Перечисленные операции доступны для всех ресурсов, вне зависимости от типа ресурса.

Ресурсы KUMA располагаются в папках. Вы можете добавлять, переименовывать, перемещать и удалять папки ресурсов.

Создание, переименование, перемещение и удаление папок с ресурсами

Ресурсы можно расположить по папкам. В левой части окна отображается структура папок: корневые папки соответствуют тенантам и содержат перечень всех ресурсов тенанта. Во всех остальных папках, вложенных в корневую, отображаются ресурсы отдельной папки. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Папки можно создавать, переименовывать, перемещать и удалять.

Чтобы создать папку:

1. Выберите в дереве папку, в которой требуется новая папка.
2. Нажмите на кнопку **Добавить папку**.

   Папка будет создана.

Чтобы переименовать папку:

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ...
3. В раскрывающемся списке ... выберите **Переименовать**.

   Название папки станет доступным для редактирования.
4. Введите новое название папки и нажмите **ENTER**.

   > Название папки не может быть пустым.

   Папка будет переименована.

Чтобы переместить папку,

Нажмите название папки и перетащите ее в требуемое место в структуре папок.

> Папки невозможно переместить из одного тенанта в другой

Чтобы удалить папку:

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ...

3. В раскрывающемся списке ... выберите **Удалить**.

   Появится окно подтверждения.

4. Нажмите на кнопку **OK**.

Папка будет удалена.

> Приложение не удаляет папки, которые содержат файлы или вложенные папки.

Создание, дублирование, перемещение, редактирование и удаление ресурсов

Вы можете создавать, перемещать, копировать, редактировать и удалять ресурсы.

Чтобы создать ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **<тип ресурса>**.
2. Выберите или создайте папку, в которую вы хотите добавить новый ресурс.

   Корневые папки соответствуют тенантам. Чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.

3. Нажмите на кнопку **Добавить <тип ресурса>**.

   Откроется окно для настройки параметров выбранного типа ресурсов. Доступные параметры зависят от типа ресурса.

4. Введите уникальное имя ресурса в поле **Название**.
5. Укажите обязательные параметры (они отмечены красной звездочкой).
6. При желании укажите дополнительные параметры (это необязательное действие).
7. Нажмите на кнопку **Сохранить**.

Ресурс будет создан и доступен для использования в службах и других ресурсах.

Чтобы переместить ресурс в новую папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **<тип ресурса>**.

2. Найдите нужный ресурс в структуре папок, а затем установите флажок рядом с ресурсом, который вы хотите переместить. Можно выбрать сразу несколько ресурсов.

   Рядом с выбранными ресурсами отобразится значок ⣿.

3. Перетащите ресурсы в нужную папку с помощью значка ⣿.

Ресурсы будут перемещены в новые папки.

> Вы можете перемещать ресурсы только в папки того тенанта, в рамках которого были созданы ресурсы. Перемещение ресурсов в папки другого тенанта недоступно.

Чтобы скопировать ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **<тип ресурса>**.

2. Найдите нужный ресурс в структуре папок, установите флажок рядом с ресурсом, который вы хотите скопировать, и нажмите на кнопку **Дублировать**.

   Отображается окно с параметрами ресурса, который вы выбрали для копирования. Доступные параметры зависят от типа ресурса.

   В поле **Название** отображается `<название выбранного ресурса> - копия`.

3. Измените нужные параметры.

4. Введите уникальное имя в поле **Название**.

5. Нажмите на кнопку **Сохранить**.

Копия ресурса будет создана.

Чтобы изменить ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **<тип ресурса>**.

2. Найдите нужный ресурс в структуре папок и выберите ресурс его.

   Отображается окно с параметрами выбранного ресурса. Доступные параметры зависят от типа ресурса.

3. Измените нужные параметры.

4. Нажмите на кнопку **Сохранить**.

Ресурс будет обновлен. Если этот ресурс используется в службе, перезапустите службу, чтобы она задействовала новые параметры.

Чтобы удалить ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **<тип ресурса>**.
2. Найдите нужный ресурс в структуре папок.
3. Установите флажок рядом с ресурсом, которые вы хотите удалить, и нажмите **Удалить**.

   Откроется окно подтверждения.
4. Нажмите на кнопку **OK**.

Ресурс будет удален.

Привязка ресурсов к службам

Вы можете привязать ресурсы (правила корреляции, правила обогащения, правила реагирования, правила агрегирования и точки назначения) к таким службам, как коллекторы и корреляторы. Доступные службы зависят от типа выбранного ресурса.

Чтобы привязать ресурс к службе:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и службы** → раздел **<имя ресурса>**.
2. Установите флажок рядом с каждым ресурсом, который вы хотите привязать, и в панели инструментов или в меню (⋮) нажмите **Привязать к сервису** → **Привязать к <название службы>**.

   Вы также можете привязать ресурс к службе при изменении параметров ресурса. Для этого нажмите на название ресурса, перейдите на вкладку **Службы** и нажмите **Привязать к сервису** → **Привязать к <название службы>**.

   > При изменении параметров правила корреляции доступна вкладка **Корреляторы**, где вы можете привязать правило к корреляторам.
3. В открывшемся окне **<название службы>** установите флажки рядом с нужными службами и нажмите **OK**.

Ресурс будет привязан к службе.

Чтобы отвязать ресурс от службы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и службы** → раздел **<имя ресурса>**.
2. Нажмите на ресурс и перейдите на вкладку **Службы**.

   > Для правил корреляции отображается вкладка **Корреляторы**.

3. Установите флажок рядом с каждой службой, от которой вы хотите отвязать ресурс.

4. Нажмите **Удалить** и подтвердите удаление привязки к службе.

   Связь ресурса со службой будет удалена.

Обновление ресурсов

Подсистема обновлений KUMA предоставляет механизмы для получения, хранения и использования ресурсов, необходимых для обработки событий и обнаружения угроз. Подсистема включает в себя два независимых механизма обновления:

- **Обновление хранилища** – механизм загрузки пакетов ресурсов с возможностью их просмотра, анализа и импорта в тенант.
- **Обновление OSMP** – автоматический механизм получения и использования ресурсов без участия пользователя и импорта вручную.

Оба механизма могут использовать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского".
- Пользовательский источник (хранилище или зеркало обновлений).

Подсистема обновлений расширяет возможности KUMA для реагирования на изменения в картине угроз и инфраструктуре. Возможность использовать систему без прямого доступа в интернет помогает обеспечить конфиденциальность данных, обрабатываемых системой.

Рабочий процесс обновления ресурсов

Чтобы обновить ресурсы, вам необходимо выполнить следующие шаги:

1. Обновить хранилище, чтобы доставить в хранилище пакеты с ресурсами. Обновление репозитория доступно в двух режимах:
   - Автоматическое обновление.
   - Обновление вручную.
2. Импортировать пакеты с ресурсами из обновленного репозитория в тенант.
3. Убедитесь, что обновленные ресурсы сопоставлены после выполнения импорта. В случае необходимости привяжите ресурсы к коллекторам, корреляторам или агентам и обновите параметры.

Обновление репозитория

"Лаборатория Касперского" регулярно выпускает пакеты с ресурсами, доступные для импорта из репозитория. Вы можете указать адрес электронной почты в параметрах задачи **Обновление хранилища**. После первого выполнения задачи KUMA начинает рассылку уведомлений о доступных для обновления пакетах на указанный адрес.

Механизм обновления репозитория позволяет извлекать пакеты, просматривать их содержимое и принимать решение о развертывании их в операционной инфраструктуре. Обновление репозитория может производиться в автоматически или вручную.

При использовании в инфраструктуре других приложений "Лаборатории Касперского", можно подключить KUMA к уже существующем зеркалам обновления.

Чтобы настроить автоматическое обновление:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Другое** нажмите **Параметры обновления**.

3. В блоке **Обновление репозитория** настройте **Период обновления данных в часах**. Значение по умолчанию – 24 часа.

4. Укажите **Источник обновления**. Доступны следующие параметры:

   - Серверы обновлений "Лаборатории Касперского".

     Вы можете посмотреть список серверов в Базе знаний.

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у системного пользователя kuma должен быть доступ для чтения к этой папке и ее содержимому.

5. Укажите **Адреса электронной почты для рассылки уведомлений** для рассылки уведомлений, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

6. Нажмите на кнопку **Сохранить**. Вскоре запустится задача обновления. Затем задача запускается по расписанию.

Чтобы запустить обновление репозитория вручную:

1. Если вы хотите выключить автоматическое обновление, в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Параметры обновления** → **Обновление репозитория** включите переключатель **Отключить автоматическое обновление**. По умолчанию этот переключатель выключен. Также вы можете запустить обновление репозитория вручную, не отключая автоматическое обновление. Запуск обновления вручную не влияет на график выполнения автоматического обновления.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - Серверы обновлений "Лаборатории Касперского".

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому.

3. Укажите **Адреса электронной почты для рассылки уведомлений** для рассылки уведомлений, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

4. Нажмите **Запустить обновление**. Таким образом, вы одновременно сохраните настройки и вручную запустите выполнение задачи **Обновление репозитория**.

Обновление OSMP

Если это поддерживается лицензией, механизм обновления OSMP автоматически получает и использует ресурсы. Обновление OSMP выполняется автоматически в фоновом режиме и не требует импорта, анализа или одобрения пакетов вручную.

После завершения обновления новые поля событий и правила корреляции становятся доступными для обработки без дополнительной настройки.

Чтобы настроить обновление OSMP:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Параметры обновления**.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - Серверы обновлений "Лаборатории Касперского".

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому. Если используется пользовательский источник, при необходимости настройте параметры прокси-сервера.

3. В блоке **Обновление OSMP** в поле **Период обновления данных в минутах** укажите период автоматической проверки и загрузки обновлений в минутах. Значение по умолчанию – 30.

4. Нажмите на кнопку **Сохранить**.

По умолчанию переключатель **Отключить автоматическое обновление** выключен, и обновление OSMP запускается автоматически в соответствии с интервалом указанным в поле **Период обновления данных в минутах**.

Если вы хотите выключить автоматическое обновление OSMP, включите переключатель **Отключить автоматическое обновление** и нажмите **Сохранить**. В этом случае автоматическая проверка обновлений и загрузка не выполняются. Чтобы запустить обновление OSMP вручную, нажмите **Запустить обновление**.

Настройка пользовательского источника с использованием Kaspersky Update Utility

Вы можете обновлять ресурсы без доступа к интернету через пользовательский источник обновления с помощью утилиты Kaspersky Update Utility.

Настройка состоит из следующих шагов:

1. Настройка пользовательского источника с помощью Kaspersky Update Utility:

   a. Установка и настройка Kaspersky Update Utility на одном из компьютеров локальной сети организации.

   b. Настройка копирования обновлений в папку общего доступа в параметрах Kaspersky Update Utility.

2. Настройка обновления репозитория KUMA из пользовательского источника.

Настройка пользовательского источника с помощью Kaspersky Update Utility:

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта Службы технической поддержки "Лаборатории Касперского".

1. В Kaspersky Update Utility включите скачивание обновлений для KUMA:

   - В разделе **Приложения** – **Контроль периметра** установите флажок рядом с KUMA, чтобы включить возможность обновления.

   - Если вы работаете с Kaspersky Update Utility через командную строку, в конфигурационном файле updater.ini в секции [ComponentSettings] добавьте следующую строку или укажите значение `true` для уже существующей строки:

     ```
     KasperskyUnifiedMonitoringAndAnalysisPlatform_XDR_1_1=true
     ```

2. В разделе **Загрузки** укажите источник обновлений. По умолчанию в качестве источника используются сервера обновления "Лаборатории Касперского".

3. В разделе **Загрузки** в группе параметров **Папки для обновлений** укажите папку общего доступа, в которую Kaspersky Update Utility будет загружать обновления. Доступны следующие параметры:

   - Укажите локальную папку на устройстве, где установлена Kaspersky Update Utility. Разверните HTTP-сервер, который будет отдавать обновления, и опубликуйте на нем эту локальную папку. В Консоли OSMP в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Обновление репозитория** → **Пользовательский источник** укажите URL к локальной папке, опубликованной на HTTP-сервере.

   - Укажите локальную папку на устройстве, где установлена Kaspersky Update Utility. Сделайте эту локальную папку доступной по сети. Примонтируйте доступную по сети локальную папку на устройстве с KUMA. В Консоли OSMP в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Обновление репозитория** → **Пользовательский источник** укажите полный путь к этой локальной папке.

Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

Экспорт ресурсов

Если для пользователя скрыты общие ресурсы, он не может экспортировать ни общие ресурсы, ни ресурсы, в которых используются общие ресурсы.

Чтобы экспортировать ресурсы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Правила корреляции**.

2. Нажмите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы** с деревом всех доступных ресурсов.

3. В поле **Пароль** введите пароль, который необходимо использовать для защиты экспортируемых данных.

4. В раскрывающемся списке **Тенант** выберите тенант, ресурсы которого вы хотите экспортировать.

5. Установите флажки рядом с ресурсами, которые вы хотите экспортировать.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы.

6. Нажмите на кнопку **Экспортировать**.

Ресурсы в защищенном паролем файле сохранятся на вашем компьютере в зависимости от настроек вашего браузера. Ресурсы секретов экспортируются пустыми.

Импорт ресурсов

Чтобы импортировать ресурсы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.

2. Нажмите **Импортировать ресурсы**.

   Откроется окно **Импортировать ресурсы**.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать импортируемые ресурсы.

4. В раскрывающемся списке **Источник импорта** выберите один из следующих вариантов:

   - **Файл**

     При выборе этого варианта необходимо указать пароль и нажать на кнопку **Импортировать**.

   - **Хранилище**

     При выборе этого варианта отображается список доступных для импорта пакетов. Рекомендуется убедиться, что дата обновления хранилища относительно недавняя и при необходимости настроить автоматическое обновление.

     Вы можете выбрать один или несколько пакетов для импорта и нажать на кнопку **Импортировать**. Зависимые ресурсы Общего тенанта будут импортированы в Общий тенант, остальные ресурсы будут импортированы в выбранный тенант. Отдельных прав для учетной записи на Общий тенант не требуется, необходимо только наличие права на импорт в выбранном тенанте.

     Импортированные ресурсы, отмеченные как **Этот ресурс входит в пакет. Его можно удалить, но он недоступен для редактирования**, можно только удалить. Если вы хотите переименовать, изменить или переместить импортированный ресурс, вам нужно сделать копию ресурса с помощью кнопки **Дублировать** и с копией выполнить нужные действия. При импорте следующих версий пакета дубликат не будет обновлен, поскольку он уже представляет собой отдельный объект.

     Импортированные ресурсы с пометкой **Этот ресурс входит в пакет**, расположенные в директории `Интеграция`, можно редактировать. Например, можно изменять фильтры исключений из правил корреляции в директории `Интеграция`. Фильтры исключений содержат списки условий, предотвращающих ложные срабатывания правил корреляции. К фильтрам исключений можно добавлять условия перед началом работы правил корреляции или во время их работы, чтобы уменьшить частоту ложных срабатываний, которая может различаться в зависимости от конкретного сетевого окружения. Фильтры исключений, предоставляемые "Лабораторией Касперского", добавлены в селекторы правил корреляции по умолчанию.

     При импорте последующих версий пакета измененные ресурсы не будут заменятся на аналогичные ресурсы из пакета, что позволит сохранить внесенные изменения. Изменения, внесенные в фильтры исключений, применяются на постоянной основе, что отличает их от временных исключений.

     Ресурсы из репозитория импортируются из репозитория на языке, указанном в параметре Локализация ресурсов KUMA в разделе Параметры Ядра KUMA.

5. Разрешите конфликты между импортированными из файла и существующими ресурсами, если они возникли. Подробнее о конфликтах ресурсов см. ниже.

   a. Если имя, тип и guid импортированных ресурсов полностью совпадает с именем, типом и guid существующего ресурса, открывается окно **Конфликты** с таблицей, в которой отображаются тип и имя конфликтующих ресурсов. Разрешите отображаемые конфликты:

      - Если вы хотите заменить существующий ресурс новым, нажмите **Заменить**.

        Нажмите **Заменить все**, чтобы заменить все конфликтующие ресурсы.

      - Если вы хотите оставить существующий ресурс, нажмите **Пропустить**.

        Для зависимых ресурсов, то есть привязанных к другим ресурсам, недоступен параметр **Пропустить**, зависимые ресурсы можно только **Заменить**.

        Нажмите **Пропустить все**, чтобы сохранить все существующие ресурсы.

   b. Нажмите на кнопку **Устранить**.

   Ресурсы импортируются в KUMA. Ресурсы секретов импортируются пустыми.

Импорт ресурсов, использующих расширенную схему событий

Если вы импортируете нормализатор, использующий одно или несколько полей расширенной схемы событий, в KUMA будет автоматически создано поле расширенной схемы, использующееся в нормализаторе.

Если вы импортируете прочие типы ресурсов, использующих в своей логике поля расширенной схемы событий, ресурсы будут успешно импортированы. Для обеспечения работы импортированных ресурсов необходимо создать соответствующие поля расширенной схемы событий в ресурсе типа "нормализатор".

Если в KUMA будет импортирован нормализатор, использующий поле расширенной схемы событий и такое поле уже существует в KUMA, будет использовано созданное ранее поле.

О разрешении конфликтов

Когда ресурсы импортируются в KUMA из файла, приложение сравнивает их с существующими ресурсами, сверяя следующие параметры:

- Имя и тип. Если имя и тип импортируемого ресурса совпадают с параметрами существующего ресурса, имя импортированного ресурса автоматически изменяется.

- идентификатор; Если идентификаторы двух ресурсов совпадают, возникает конфликт, который должен разрешить пользователь. Такая ситуация может возникнуть, когда вы импортируете ресурсы на тот же сервер KUMA, с которого они были экспортированы.

При разрешении конфликта вы можете либо *заменить существующий ресурс* импортированным, либо *оставить существующий ресурс*.

Некоторые ресурсы связаны между собой: например, в некоторых типах коннекторов обязательно нужно указывать секрет коннектора. Секреты также импортируются, если они привязаны к коннектору. Такие связанные ресурсы экспортируются и импортируются вместе.

Особенности импорта:

1. Ресурсы импортируются в выбранный тенант.

2. Если связанный ресурс находился в Общем тенанте, при импорте он снова будет в Общем тенанте.

3. В окне **Конфликты** в столбце **Родительский объект** всегда отображается самый верхний родительский ресурс из выбранных при импорте.

4. Если во время импорта возникает конфликт, и вы выбираете замену существующего ресурса новым, все связанные с ним ресурсы также будут автоматически заменены импортированными ресурсами.

Известные ошибки:

1. Привязанный ресурс попадает в тенант, указанный при импорте, а не в Общий тенант, как указано в окне **Конфликты**, при следующих условиях:

   a. привязанный ресурс изначально находится в Общем тенанте;

   b. в окне **Конфликты** вы выбираете **Пропустить** для всех родительских объектов привязанного ресурса из Общего тенанта;

   c. привязанный ресурс из Общего тенанта оставляете для замены.

2. После выполнения импорта в фильтре у категорий не указан тенант при следующих условиях:

   a. фильтр содержит привязанные категории активов из разных тенантов;

   b. имена категорий активов одинаковы;

   c. вы импортируете этот фильтр с привязанными категориями активов на новый сервер.

3. В Тенант 1 дублируется имя категории активов при следующих условиях:

   a. в Тенант 1 у вас есть фильтр с привязанными категориями активов из Тенант 1 и Общего тенанта;

   b. имена привязанных категорий активов одинаковы;

   c. вы импортируете такой фильтр из Тенант 1 в Общий тенант.

4. Невозможно импортировать конфликтующие ресурсы в один тенант.

   Ошибка *Невозможно импортировать конфликтующие ресурсы в один тенант* означает, что в импортируемом пакете есть конфликтующие ресурсы из разных тенантов и их нельзя импортировать в Общий тенант.

   Решение: Выберите для импорта пакета другой тенант, не Общий. Тогда при импорте ресурсы, изначально расположенные в Общем тенанте, будут импортированы в Общий тенант, а ресурсы из другого тенанта – в выбранный при импорте тенант.

5. Только Главный администратор может импортировать категории в Общий тенант.

   Ошибка *Только Главный администратор может импортировать категории в Общий тенант* означает, что в импортируемом пакете есть ресурсы с привязанными общими категориями активов. Категории или ресурсы с привязанными общими категориями активов можно увидеть в журнале Ядра KUMA. Путь к журналу Ядра:

   /opt/kaspersky/kuma/core/log/core

Решение: Выберите один из следующих вариантов:

- Уберите из импорта ресурсы, к которым привязаны общие категории: снимите флажок рядом с соответствующими ресурсами.
- Выполните импорт под учетной записью пользователя с правами Главного администратора.

6. Только главный администратор может импортировать ресурсы в Общий тенант.

   Ошибка *Только Главный администратор может импортировать ресурсы в Общий тенант* означает, что в импортируемом пакете есть ресурсы с привязанными общими ресурсами. Ресурсы с привязанными общими ресурсами можно увидеть в журнале Ядра KUMA. Путь к журналу Ядра:

   /opt/kaspersky/kuma/core/log/core

   Решение: Выберите один из следующих вариантов:

   - Уберите из импорта ресурсы, к которым привязаны ресурсы из Общего тенанта, и сами общие ресурсы: снимите флажок рядом с соответствующими ресурсами.
   - Выполните импорт под учетной записью пользователя с правами Главного администратора.

Управление тегами

Для работы с ресурсами в веб-интерфейсе KUMA предусмотрена возможность добавлять теги для ресурсов. Вы можете выполнять поиск нужного компонента, а также управлять тегами, назначать теги или отменять назначение тегов.

Невозможно добавлять теги в ресурсы, которые создаются из интерфейса других ресурсов. Теги можно добавлять только из карточки самого ресурса. Также невозможно добавлять теги к ресурсу, недоступному для редактирования.

Управление тегами

Список тегов отображается в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Теги** и представлен в виде таблицы со столбцами **Название**, **Тенант**, **Использовано в ресурсах**.

В таблице **Теги** вы можете выполнять следующие действия:

- Сортировать теги по полям **Название**, **Использовано в ресурсах**.
- Фильтровать значения поля **Тенант**.
- Осуществлять поиск тега по полю **Название**.
- Переходить к списку ресурсов по выбранному тегу.

Добавление тега

Чтобы добавить тег:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** и выберите ресурс.
2. В панели над таблицей нажмите **Добавить**.
3. В поле **Теги** выбранного ресурса добавьте новый тег или выберите тег из списка.
4. Нажмите на кнопку **Создать**.

   Новый тег будет добавлен.

Вы также можете добавлять теги из уже существующих.

При добавлении тега следует учитывать следующие особенности:

- Вы можете добавить несколько тегов.
- Тег может содержать буквы различных алфавитов (например, символы кириллицы, латиницы или греческого алфавита), цифры, знак нижнего подчеркивания и пробел.
- Тег не может содержать другие специальные символы, кроме нижнего подчеркивания и пробела.
- Вы можете вводить тег в любом регистре, но после сохранения тег будет всегда отображаться в нижнем регистре.
- Тег наследует тенант ресурса, в котором используется.
- Тег является частью ресурса и существует, пока существует ресурс, в котором тег был создан или используется.
- Теги уникальны в рамках тенанта.
- Теги импортируются или экспортируются вместе с ресурсом как часть ресурса.

Поиск по тегам

В разделе **Ресурсы** вы можете осуществить поиск ресурсов:

- По тегам.
- По наименованию ресурсов.

Поиск осуществляется по всем типам ресурсов и служб.

В результате поиска отображается список ресурсов и служб.

Чтобы найти нужные ресурсы по тегам:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** и выберите ресурс.
2. В таблице ресурса выберите столбец **Теги**.
3. В появившемся поле **Поиск** введите или выберите название тега.

   Поиск по тегу в самом ресурсе и в списке ресурсов осуществляется как при полном, так и частичном совпадении введенного текста с названием тега.

Отображается список ресурсов, если в этих ресурсах используется указанный тег.

В списке ресурсов вы можете выполнять следующие действия:

- Сортировать список по наименованию, типу ресурса или службы.
- Фильтровать ресурсы или службы по типу ресурса или службы, тегу.
- Назначать теги или отменять назначение тегов.

Отображение тегов при добавлении зависимых ресурсов

При добавлении зависимого ресурса в раскрывающемся списке отображаются теги этого ресурса в разделе **Параметры фильтра**.

Теги ресурса, которые не помещаются в одну строку, скрываются. На наличие скрытых тегов указывает специальный признак.

Раскрывающийся список можно фильтровать по названию ресурса и по тегам ресурса.

Назначение тегов или отмена назначения тегов

Чтобы назначить теги ресурсу или отменить назначение тегов ресурсу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы**.
2. Выберите вкладку **Список**.
3. В столбце **Название** установите флажки рядом с нужными ресурсами.
4. В панели над списком выберите вкладку **Теги**.
5. Нажмите на кнопку **Привязать** или **Отвязать**, выберите нужные теги или создайте тег.

   Выбранные теги будут назначены ресурсам или назначение тегов ресурсам будет удалено.

   Вы также можете привязать или отвязать теги в карточке ресурса.

Точки назначения

Точки назначения задают сетевые параметры для передачи нормализованных событий. Точки назначения используются в коллекторах и корреляторах для описания того, куда передавать обработанные события. В основном, в роли точек назначения выступают коррелятор и хранилище.

Параметры точек назначения указываются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:

- **internal** – используются для приема данных от сервисов KUMA по протоколу internal.
- **nats-jetstream** – используется для коммуникации через NATS.
- **tcp** – используется для связи по протоколу TCP.
- **udp** – используются для связи по протоколу UDP.
- **http** – используется для связи по протоколу HTTP.
- **diode** – используется для передачи событий с помощью диода данных.
- **kafka** – используется для коммуникаций с помощью kafka.
- **file** – используется для записи в файл.
- **storage** – используется для передачи данных в хранилище.
- **correlator** – используется для передачи данных в коррелятор.

Точка назначения, тип internal

Точки назначения с типом **internal** используются для приема данных от сервисов KUMA по протоколу internal. Вы можете передавать следующие данные по протоколу internal:

- Внутренние данные, такие как маршруты событий.
- Файловые атрибуты. Если при создании коллектора на шаге Транспорт мастера установки, вы указали коннектор с типом file, 1c-xml или 1c-log, на шаге Парсинг событий в таблице **Сопоставление** вы можете передать в поле события KUMA название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:
  - `$kuma_fileSourceName` – передать в поле события KUMA название обрабатываемого коллектором файла.
  - `$kuma_fileSourcePath` – передать в поле события KUMA путь к обрабатываемому коллектором файлу.

  При использовании **коннектора с типом file**, **1c-xml** или **1c-log**, новые переменные в нормализаторе будут работать только с **точками назначения с типом internal**.

Доступные параметры точки назначения с типом **internal** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип.	Тип точки назначения: **internal**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >< номер порта >`. IPv6-адреса можно указать в формате `[< IPv6-адрес >%< интерфейс >:< номер порта >`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. KUMA не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша 🖊.

Параметр	Описание
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

Параметр	Описание
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде. d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип nats-jetstream

Тип **nats-jetstream** используется для коммуникации через NATS.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **nats-jetstream**.
URL	Обязательный параметр. URL, с которым необходимо установить связь.
Топик	Обязательный параметр. Тема сообщений NATS. Должно содержать символы Юникода.

Параметр	Описание
Разделитель	Используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
Авторизация	Тип авторизации при подключении к указанному URL Доступны следующие значения: • **выключена** – значение по умолчанию. • **обычная** – при выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. **Добавить секрет** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Идентификатор кластера	Идентификатор кластера NATS.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.

Параметр	Описание

Режим TLS	Использование шифрования TLS. Доступные значения:
	• **Выключено**: значение по умолчанию, не использовать шифрование TLS.
	• **Включено –** использовать шифрование, но без верификации сертификата.
	• **С проверкой** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
	• **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.
	Создание сертификата, подписанного центром сертификации
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Open Single Management Platform (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< общее имя устройства центра сертификации >" -out ca.crt`
	3. Создайте закрытый ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< общее имя хоста сервера Open Single Management Platform >" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Open Single Management Platform в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	При использовании TLS невозможно указать IP-адрес в качестве URL.

Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 c`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип tcp

Тип **tcp** используется для связи по протоколу TCP.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **tcp**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6. При использовании адресов IPv6 необходимо также указывать интерфейс в формате `[адрес%интерфейс]:порт`. Например: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другой службы или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Режим TLS	Использование шифрования TLS с использованием сертификатов в формате pem x509. Доступные значения: • **Выключено**: не использовать шифрование TLS. Значение по умолчанию. • **Включено** – использовать шифрование, но без верификации сертификатов. • **Нестандартный CA** означает, что используется шифрование и проверяется сертификат, предоставленный вами в виде файла. При выборе этого значения отображается дополнительный параметр **Нестандартный CA**. С помощью этого параметра необходимо указать сертификат. • **Нестандартный PFX** означает, что используется шифрование и проверяется сертификат, предоставленный вами в формате PFX. При выборе этого значения отображается дополнительный параметр **PFX секрет**. С помощью этого параметра необходимо указать сертификат. При использовании TLS невозможно указать IP-адрес в качестве URL.
Нестандартный CA	В этом поле можно выбрать секрет типа certificate, который содержит файл сертификата. Вы можете выбрать существующий секрет или создать новый. Чтобы создать новый, выберите вариант **Создать**, затем в открывшемся окне загрузите файл TLS-сертификата.
PFX секрет	В этом поле можно выбрать секрет типа pfx, который содержит файл сертификата. Можно выбрать существующий секрет или создать новый. Чтобы создать новый, выберите вариант **Создать**, затем в открывшемся окне загрузите файл PFX, содержащий TLS-сертификат.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип udp

Точки назначения с типом **udp** используются для связи по протоколу UDP. Доступные параметры точки назначения с типом **udp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **udp**. Обязательный параметр.

Параметр	Описание
URL	URL, с которым требуется установить связь. Поддерживаются следующие форматы URL: • `< имя устройства >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >< номер порта >`. IPv6-адреса можно указать в формате `[< IPv6-адрес >%< интерфейс >:< номер порта >`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL и удалить URL. Вы не можете сохранить ресурс или сервис если в поле **URL** есть знак табуляции или пробел. Для добавления URL нажмите на кнопку **+ Добавить**. Для удаления URL нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов. • **С верификацией** – использовать шифрование TLS с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и помещаются на сервер Ядра KUMA в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.
Политика выбора URL	Способ определения URL, на которые события отправляются в первую очередь, если вы добавили несколько URL в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL до тех пор, пока URL принимает события. Если URL станет недоступным, события будут отправляться на другой случайно выбранный доступный URL. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL. Если URL станет недоступным, события будут отправляться на следующий добавленный доступный URL. Если первый добавленный URL снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL. Этот способ определения URL не гарантирует равномерного распределения событий по URL, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.

Параметр	Описание
Разделитель	Символ, определяющий границу между событиями: • \n; • \t; • \0. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

Параметр	Описание
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде. d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип http

Тип **http** используется для связи по протоколу HTTP.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **http**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

Параметр	Описание
Авторизация	Тип авторизации при подключении к указанному URL. Доступны следующие значения: • **выключена** – значение по умолчанию. • **обычная** – при выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. **Добавить секрет** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другой службы или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.

Параметр	Описание

Режим TLS	Использование шифрования TLS. Доступные значения:
	• **Выключено**: значение по умолчанию, не использовать шифрование TLS.
	• **Включено –** использовать шифрование, но без верификации сертификата.
	• **С проверкой** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
	• **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.
	Создание сертификата, подписанного центром сертификации
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Open Single Management Platform (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< общее имя устройства центра сертификации >" -out ca.crt`
	3. Создайте закрытый ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< общее имя хоста сервера Open Single Management Platform >" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Open Single Management Platform в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	При использовании TLS невозможно указать IP-адрес в качестве URL.

Политика выбора URL	В раскрывающемся списке можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько. Доступные значения: • **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL. • **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него. • **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется \n.
Path	Путь, который необходимо добавить для URL-запроса. Например, если указать путь `/input`, а в качестве URL ввести `10.10.10.10`, то от точки назначения будут исходить запросы `10.10.10.10/input`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 c`.
Количество обработчиков	Количество служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Путь проверки работоспособности	URL для отправки запросов для получения данных о работоспособности системы, с которой устанавливает связь ресурс точки назначения.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Проверка работоспособности отключена	Флажок, который отключает проверку работоспособности.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.

Параметр	Описание
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип diode

Тип **diode** используется для передачи событий с помощью диода данных.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **diode**.

Параметр	Описание
Директория, из которой диод данных получает события	Обязательный параметр. Директория, откуда диод данных перемещает события. Путь может содержать до 255 символов Юникода. **Ограничения при использовании префиксов к путям на серверах Windows** На серверах Windows необходимо указывать абсолютные пути к директориям. Невозможно использовать директории, названия которых соответствуют указанным ниже регулярным выражениям: • `^[a-zA-Z]:\\Program Files` • `^[a-zA-Z]:\\Program Files \(x86\)` • `^[a-zA-Z]:\\Windows` • `^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA` **Ограничения при использовании префиксов к путям на серверах Linux** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/`

Параметр	Описание
Временная директория	Директория, в которой события готовятся для передачи диоду данных. События хранятся в файле по истечении времени ожидания (по умолчанию 10 секунд) или при переполнении буфера. Подготовленный файл перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**. В качестве названия файла с событиями используется хеш-сумма (SHA256) содержимого файла. Временная директория не должна совпадать с директорией, из которой диод данных получает события.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**. Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`. Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.

Параметр	Описание
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип kafka

Тип **kafka** используется для коммуникаций с помощью kafka.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **kafka**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`). Вы можете добавить несколько адресов, нажав на кнопку URL.
Топик	Обязательный параметр. Тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".

Параметр	Описание
Разделитель	Используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
Авторизация	Тип авторизации при подключении к указанному URL. Доступны следующие значения: • **выключена** – значение по умолчанию. • **PFX** – сертификат должен быть сгенерирован с закрытым ключом в формате контейнера PKCS#12 в доверенном центре сертификации. Затем сертификат нужно экспортировать из хранилища и загрузить его в Консоли KUMA в виде PFX-секрета. • **Добавить PFX-секрет** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**. • **обычная** – требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. **Добавить секрет** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другой службы или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.

Параметр	Описание

Режим TLS	Использование шифрования TLS. Доступные значения:
	• **Выключено –** значение по умолчанию, не использовать шифрование TLS.
	• **Включено** – использовать шифрование, но без верификации сертификата.
	• **С проверкой** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
	• **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.
	Создание сертификата, подписанного центром сертификации
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Open Single Management Platform (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< общее имя устройства центра сертификации >" -out ca.crt`
	3. Создайте закрытый ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< общее имя хоста сервера Open Single Management Platform >" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Open Single Management Platform в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	При использовании TLS невозможно указать IP-адрес в качестве URL.

Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 c`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип файла

Тип **file** используется для записи в файл.

> При удалении точки назначения типа file, используемой в какой-либо службе, эту службу необходимо перезапустить.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **file**.

Параметр	Описание
URL	Обязательный параметр. Путь к файлу, в который необходимо записать события. **Ограничения при использовании префиксов к путям файлов** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/`
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется \n.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип storage

Тип **storage** используется для передачи данных в хранилище.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **storage**.

Параметр	Описание
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`). Вы можете добавить несколько адресов, нажав на кнопку **URL**. В поле **URL** поддерживается поиск служб по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям: • `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям служб. • `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам служб, а второе значение используется для поиска по порту. • `:<значение>` – поиск ведется по порту.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Прокси-сервер	Раскрывающийся список для выбора прокси-сервера.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Политика выбора URL	Раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько: • **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL. • **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него. • **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Тип correlator

Тип **correlator** используется для передачи данных в коррелятор.

Вкладка Основные параметры

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип.	Обязательный параметр. Тип точки назначения, **correlator**.

Параметр	Описание
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`). Вы можете добавить несколько адресов, нажав на кнопку **URL**. В поле **URL** поддерживается поиск служб по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям: • `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям служб. • `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам служб, а второе значение используется для поиска по порту. • `:<значение>` – поиск ведется по порту.
Описание	Описание ресурса: до 4000 символов Юникода.

Вкладка Дополнительные параметры

Параметр	Описание
Прокси-сервер	Раскрывающийся список для выбора прокси-сервера.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Политика выбора URL	Раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько: • **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL. • **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него. • **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

Параметр	Описание
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или создать новый фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам и корреляторам.

Для привязки точки назначения к службе, нажмите на кнопку **Привязать к службе** → **Привязать к <название_службы>**. В открывшемся окне выберите одну или несколько служб и нажмите **OK**. Точка назначения будет привязана к выбранным службам.

При необходимости вы можете удалить связь между точкой назначения и службой. Для этого нужно установить флажок рядом с нужной службой, нажать **Удалить** и подтвердить удаление привязки к службе.

Предустановленные точки назначения

В поставку OSMP включены перечисленные в таблице ниже точки назначения.

Предустановленные точки назначения

Название точки назначения	Описание
[OOTB] Correlator	Отправляет события в коррелятор.
[OOTB] Storage	Отправляет события в хранилище.

Нормализаторы

Нормализаторы предназначены для приведения исходных событий, которые поступают из разных источников в разных форматах, к модели данных событий KUMA. Нормализованные события становятся доступны для обработки другими ресурсами и сервисами KUMA.

Нормализатор состоит из *основного* и необязательных *дополнительных правил парсинга событий*. С помощью создания основного и множества дополнительных правил парсинга можно реализовать сложную логику обработки событий. Данные передаются по древовидной структуре правил парсинга в зависимости от условий, заданных в параметре **Условия дополнительной нормализации**. Последовательность создания правил парсинга имеет значение: событие обрабатывается последовательно и последовательность обработки обозначена стрелками.

Нормализация событий теперь доступна в следующих вариантах:

- 1 коллектор - 1 нормализатор

  Рекомендуется использовать такой способ, если у вас много событий одного типа или много IP-адресов, откуда могут приходить события одного типа. Можно настроить один коллектор только с одним нормализатором и это будет оптимально с точки зрения производительности.

- 1 коллектор - несколько нормализаторов с привязкой к IP

  Такой способ доступен для коллекторов с коннектором типа UDP, TCP, HTTP. Если в коллекторе на шаге Транспорт указан коннектор UDP, TCP, HTTP, на шаге Парсинг событий на вкладке Настройки парсинга вы можете задать несколько IP-адресов и указать, какой нормализатор использовать для событий, поступающих с заданных адресов. Доступны следующие типы нормализаторов: `json`, `cef`, `regexp`, `syslog`, `csv`, `kv`, `xml`. Для нормализаторов типа `syslog` и `regexp` вы можете задать дополнительные условия нормализации в зависимости от значения поля DeviceProcessName.

Нормализатор создается в несколько этапов:

1. **Подготовка к созданию нормализатора**

   Нормализатор можно создать в Консоли OSMP:

   - В разделе **Мониторинг** → **Ресурсы** → **Нормализаторы**.
   - При создании коллектора на шаге **Парсинг событий**.

   Затем в нормализаторе необходимо создать правила парсинга.

2. **Создание основного правила парсинга событий**

   Основное правило парсинга создается нажатием на кнопку **Добавить парсинг событий**. При этом открывается окно **Парсинг событий**, в котором вы можете задать параметры основного правила парсинга:

   - Задать параметры парсинга событий.
   - Задать параметры обогащения событий.

   Основное правило парсинга событий отображается в нормализаторе в виде темного кружка. Параметры основного правила парсинга можно просмотреть или изменить, нажав на его кружок. При наведении курсора мыши на кружок отображается знак плюса. Нажмите на него, чтобы добавить правила парсинга.

   Название основного правила парсинга используется в KUMA в качестве названия нормализатора.

3. **Создание дополнительных правил парсинга событий**

   При нажатии на значок плюса, который отображается при наведении указателя мыши на кружок или блок, обозначающий нормализатор событий, откроется окно **Дополнительный парсинг событий**, в котором вы можете задать параметры дополнительного правила парсинга:

   - Определить условия, при которых данные будут поступать в новый нормализатор.
   - Задать параметры парсинга событий.
   - Задать параметры обогащения событий.

   Дополнительное правило парсинга событий отображается в нормализаторе виде темного блока. В блоке отображаются условия срабатывания правила дополнительного парсинга, имя правила дополнительного парсинга и поле события. Когда это поле события доступно, данные передаются в нормализатор. Параметры дополнительного правила парсинга можно просмотреть или изменить, нажав его блок.

Если навести курсор мыши на правило дополнительного нормализатора, появится кнопка с плюсом. Вы можете нажать на эту кнопку, чтобы создать дополнительное правило парсинга событий. С помощью кнопки со значком корзины нормализатор можно удалить.

4. **Завершение создания нормализатора**

   Создание нормализатора завершается нажатием кнопки **Сохранить**.

В верхнем правом углу в поле поиска можно искать дополнительные правила парсинга по названию.

Для ресурсов нормализатора в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. Если требуется изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе Консоли OSMP **Мониторинг** → **Ресурсы** → **Нормализаторы**.

Параметры парсинга событий

При создании правил парсинга событий в окне параметров нормализатора на вкладке **Схема нормализации** вы можете настроить правила приведения поступающих событий к формату KUMA.

Чтобы определить параметры парсинга событий:

1. В поле **Версия ресурса в репозитории "Лаборатории Касперского"** указывается номер версии события.

   Это поле невозможно изменить. Доступно только для ресурсов, предоставляемых "Лабораторией Касперского" и используется для управления обновлением ресурсов.

2. В поле **Имя** (обязательное поле) введите уникальное имя правила парсинга. Имя должно содержать от 1 до 128 символов Юникода. Название основного правила парсинга будет использоваться в качестве названия нормализатора.

3. В поле **Тенант** (обязательное поле) введите имя тенанта, которому принадлежит ресурс.

   Этот параметр недоступен для дополнительных правил парсинга.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требующие заполнения.

   Доступный метод парсинга: json

   Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

   При обработке файлов с иерархически выстроенными данными можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

   Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы некорректно.

В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и, следовательно, в дополнительный нормализатор передается обрабатываемое событие целиком.

В качестве разделителя строк могут выступать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

5. В раскрывающемся списке **Сохранить сырое событие** укажите, надо ли сохранять сырое событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не сохранять** – не сохранять сырое событие. Это значение используется по умолчанию.
   - **При возникновении ошибок** – сохранять сырое событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке службы. В этом случае каждый раз, когда у события есть непустое поле `Raw`, это означает, что возникла проблема.

     > Если поля с названиями `*Address` или `*Date*` не соответствуют правилам нормализации, такие поля игнорируются. При этом не возникает ошибка нормализации и значения полей не попадают в поле `Raw` нормализованного события, даже если был указан параметр **Сохранить сырое событие** → **При возникновении ошибок**.

   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

   Этот параметр недоступен для дополнительных правил парсинга.

6. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля сырого события в нормализованном событии, если для них не были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события `Extra`. Нормализованные события можно искать и фильтровать по данным, хранящимся в поле `Extra`.

   Фильтрация по данным из поля события Extra

   Условия для фильтров по данным из поля события **Extra**:

   - Условие – **Если**.
   - Левый операнд – **поле события**.
   - В поле события вы можете указать одно из следующих значений:
     - Поле **Extra**.
     - Значение из поля Extra в следующем формате:

       `Extra.<название поля>`

       Например, `Extra.app`.

       Значение этого типа указывается вручную.
     - Значение из массива, записанного в поле **Extra**, в следующем формате:

       `Extra.<название поля>.<элемент массива>`

Например, `Extra.array.0`.

Нумерация значений в массиве начинается с 0.

Значение этого типа указывается вручную.

Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

По умолчанию поля не сохраняются.

7. В поле **Описание** укажите описание ресурса: до 4000 символов Юникода.

   Этот параметр недоступен для дополнительных правил парсинга.

8. При необходимости в поле **Примеры событий** укажите пример данных, которые вы хотите обработать.

   Этот параметр недоступен для методов парсинга **netflow5**, **netflow9**, **sflow5**, **ipfix**, **sql**.

   Поле **Примеры событий** заполняется данными, полученными из сырого события, если парсинг события был выполнен успешно и тип полученных из сырого события данных совпадает с типом поля KUMA.

   Например, значение "192.168.0.1", заключенное в кавычки, не будет отображено в поле SourceAddress, при этом значение 192.168.0.1 будет отображено в поле **Примеры событий**.

9. В таблице **Сопоставление** настройте сопоставление полей сырого события с полями событий в формате KUMA:

   a. В столбце **Исходные данные** укажите название поля сырого события, которое вы хотите преобразовать в поле события KUMA.

      Подробнее о формате полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

      Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором при нажатии на кнопку **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

      Доступные преобразования

      Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

      Доступные преобразования:

      - **lower** – используется для перевода всех символов значения в нижний регистр
      - **upper** – используется для перевода всех символов значения в верхний регистр
      - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
      - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.
- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

Рекомендации для полей столбцов KUMA

Рекомендуется настроить сопоставление для следующих полей KUMA. Иначе вы не сможете просматривать наблюдаемые объекты в деталях алертов и инцидентов.

Рекомендуемые поля KUMA зависят от типов наблюдаемых объектов:

- Для наблюдаемых объектов типа MD5 и SHA256:
  - FileHash
- Для наблюдаемых объектов типа URL:
  - RequestUrl
- Для наблюдаемых объектов типа IP-адреса:
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress

    - DeviceAddress
    - SourceTranslatedAddress
    - SourceAddress
  - Для наблюдаемых объектов типа Доменное имя:
    - DestinationDnsDomain
    - DeviceDnsDomain
    - DeviceNtDomain
    - DestinationNtDomain
    - SourceDnsDomain
    - SourceNtDomain
  - Для наблюдаемых объектов типа UserName:
    - DestinationUserName
    - SourceUserName
  - Для наблюдаемых объектов типа HostName:
    - DestinationHostName
    - DeviceHostName
    - SourceHostName

c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с `DeviceCustom*` и `Flex*`, в поле **Подпись** можно добавить уникальную пользовательскую метку.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

Чтобы KUMA могла выполнить обогащение событий данными про активы, и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам необходимо настроить сопоставление полей для адреса устройства и имени устройства в зависимости от назначения актива. Например, сопоставление для SourceAddress и SourceHostName, или DestinationAddress и DestinationHostName. В результате обогащения в карточке события появится поле SourceAssetID или DestinationAssetID и ссылка, по которой можно будет перейти в карточку актива. Также в результате обогащения сведения об активе будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля сырого события в поле события KUMA.

Если размер поля события KUMA оказывается меньше длины помещаемого в него значения, значение обрезается до размера поля события.

Расширенная схема события

При нормализации событий, помимо полей стандартной схемы событий KUMA, могут быть использованы поля расширенной схемы событий. Информация о типах полей расширенной схемы событий приведена в таблице ниже.

Использование значительного количества уникальных полей расширенной схемы событий может привести к снижению производительности системы, увеличению объема дискового пространства, необходимого для хранения событий, сложности восприятия данных.

Рекомендуется предварительно продумать и сформировать минимально необходимый набор дополнительных полей расширенной схемы событий и использовать его в нормализаторах и корреляции.

Для использования полей расширенной схемы событий необходимо выполнить следующее:

- открыть существующий или создать нормализатор событий;
- заполнить основные параметры нормализатора;
- нажать на кнопку **Добавить строку**;
- в параметре **Исходные данные** указать название исходного поля в сыром событии;
- в параметре **Поле KUMA** указать имя создаваемого поля расширенной схемы событий, см. таблицу далее. Также можно использовать одно из существующих полей расширенной схемы событий.

Поля расширенной модели данных нормализованного события

Название поля Указывается в параметре Поле KUMA	Тип данных	Доступность в нормализаторе	Описание
S.<имя поля>	Строка	Все типы	Поле с типом `Строка`
N.<имя поля>	Число	Все типы	Поле с типом `Число`
F.<имя поля>	Число с плавающей точкой	Все типы	Поле с типом `Число с плавающей точкой`
SA.<имя поля>	Массив строк	KV, JSON	Поле с типом `Массив строк`. Порядок элементов массива соответствует порядку элементов сырого события.
NA.<имя поля>	Массив целых чисел	KV, JSON	Поле с типом `Массив целых чисел`. Порядок элементов массива соответствует порядку элементов сырого события.
FA.<имя поля>	Массив чисел с плавающей точкой	KV, JSON	Поле с типом `Чисел с плавающей точкой`. Порядок элементов массива соответствует порядку элементов сырого события.

Префиксы `S.`, `N.`, `F.`, `SA.`, `NA.`, `FA.` обязательны при создании полей расширенной схемы событий, префиксы должны использовать только заглавные буквы.

Вместо `<имя поля>` необходимо задать имя поля. В имени поля допустимо использовать символы английского алфавита, числа. Использование символа "пробел" не допускается.

- Нажмите на кнопку **OK**.
- Нажмите на кнопку **Сохранить** для завершения редактирования нормализатора событий.

Нормализатор сохранен, дополнительное поле создано. После сохранение нормализатора дополнительное поле может быть использовано в других нормализаторах.

Примечание: в случае, если данные, находящиеся в поля сырого события, не соответствуют типу поля KUMA, то в процессе нормализации событий значение не будет сохранено. Например, строка `test` не может быть помещена в `числовое` поле KUMA DeviceCustomNumber1.

С точки зрения нагрузки на сервер хранения при операциях поиска событий, подготовки отчетов и других операций с событиями в хранилище наиболее предпочтительными являются поля схемы событий KUMA, затем идут поля расширенной схемы событий, затем поля Extra.

Расширенная схема события

Вы можете использовать поля расширенной схемы событий в нормализаторах для нормализации событий и в других ресурсах KUMA, например, в качестве полей виджетов или для фильтрации и поиска событий. Список всех полей расширенной схемы событий, существующих в KUMA, доступен в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Поля расширенной схемы событий**. Список полей расширенной схемы событий единый для всех тенантов.

В верхней части раздела показан номер версии полей расширенной схемы событий. Эта версия используется для управления обновлением полей расширенной схемы событий.

Просматривать таблицу полей расширенной схемы событий могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Чтение общих ресурсов, Редактирование общих ресурсов.

Таблица **Поля расширенной схемы событий** содержит следующие данные:

- **Тип** – тип данных поля расширенной схемы событий.

  Доступные типы данных

Тип	Доступность в нормализаторе	Тип данных
S	Все типы	Строка.
N	Все типы	Число.
F	Все типы	Число с плавающей точкой.
SA	KV, JSON	Массив строк. Порядок элементов массива соответствует порядку элементов сырого события.
NA	KV, JSON	Массив целых чисел. Порядок элементов массива соответствует порядку элементов сырого события.
FA	KV, JSON	Массив чисел с плавающей точкой. Порядок элементов массива соответствует порядку элементов сырого события.

- **Имя поля** – имя поля расширенной схемы событий, без типа.

  Вы можете нажать на имя, чтобы изменить параметры поля расширенной схемы событий.

- **Статус** – возможность использовать поле расширенной схемы событий в ресурсах.

  Вы можете перевести переключатель в положение **Включено** или **Выключено**, чтобы разрешить или запретить использование этого поля расширенной схемы событий в новых ресурсах. При этом выключенное поле все еще будет использоваться в уже работающих конфигурациях ресурсов, пока вы не удалите его из конфигурации вручную, а также будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

  Выключить использование поля расширенной схемы событий может только пользователь с ролью Главный администратор.

- **Дата обновления** – дата и время последнего изменения поля расширенной схемы событий.

- **Создал** – имя пользователя, который создал поле расширенной схемы событий.

- **Зависимости** – количество ресурсов KUMA, макетов панели мониторинга, отчетов, пресетов и наборов полей для поиска источников событий, использующих поле расширенной схемы событий.

  Вы можете нажать на число, чтобы открыть панель с таблицей всех ресурсов и других объектов KUMA, в которых используется это поле. Для каждой зависимости в таблице отображается название, тенант (только для ресурсов) и тип. Зависимости в таблице отсортированы по названию. Вы можете нажать на название зависимости, чтобы перейти на ее страницу (кроме макетов панели мониторинга, пресетов и сохраненных запросов пользователей).

  Вы можете просмотреть зависимости поля расширенной схемы событий только от тех ресурсов и сущностей, к тенантам которых у вас есть доступ. Если у вас нет доступа к тенанту, соответствующие ресурсы не будут отображаться в таблице, но будут учитываться в количестве зависимостей.

- **Описание** – текстовое описание поля.

По умолчанию таблица полей расширенной схемы событий отсортирована по убыванию даты обновления. При необходимости вы можете отсортировать таблицу, нажав на заголовок столбца и выбрав **По возрастанию** или **По убыванию**, а также воспользоваться контекстным поиском по имени поля.

По умолчанию в KUMA автоматически добавляются следующие служебные поля расширенной схемы событий:

- `KL_EventRoute`, тип `S` – предназначено для хранения информации о маршруте события.

  Вы можете использовать это поле в нормализаторах, в качестве ключа или значения в активных листах, в правилах обогащения, в качестве поля запроса в правилах сбора и анализа данных, в корреляционных правилах. Вы не можете использовать это поле для детектирования источников событий.

- Следующие поля добавлены в корреляционное событие:

  - `KL_CorrelationRulePriority`, тип `N`;
  - `KL_SourceAssetDisplayName`, тип `S`;
  - `KL_DestinationAssetDisplayName`, тип `S`;
  - `KL_DeviceAssetDisplayName`, тип `S`;
  - `KL_SourceAccountDisplayName`, тип `S`;
  - `KL_DestinationAccountDisplayName`, тип `S`.

  Вы можете использовать эти служебные поля для поиска событий.

Вы не можете изменять, удалять, экспортировать и отключать служебные поля. Все поля расширенной схемы событий с префиксом `KL_` являются служебными и управляются только с серверов "Лаборатории Касперского". Не рекомендуется использовать префикс `KL_` в имени при добавлении новых полей расширенной схемы событий.

Добавление полей расширенной схемы событий

Пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Редактирование общих ресурсов могут добавлять новые поля расширенной схемы событий.

Чтобы добавить поле расширенной схемы событий:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Поля расширенной схемы событий**.

   Откроется окно **Поля расширенной схемы событий**.

3. Нажмите на кнопку **Добавить** в верхней части таблицы.

   Откроется панель **Создание расширенной схемы**.

4. Включите или выключите переключатель **Статус**, чтобы разрешить или запретить использовать это поле расширенной схемы событий в ресурсах.

   По умолчанию переключатель включен. Выключенное поле все еще будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

5. В поле **Тип** выберите тип данных поля расширенной схемы событий.

   Доступные типы данных

Тип	Доступность в нормализаторе	Тип данных
S	Все типы	Строка.
N	Все типы	Число.
F	Все типы	Число с плавающей точкой.
SA	KV, JSON	Массив строк. Порядок элементов массива соответствует порядку элементов сырого события.
NA	KV, JSON	Массив целых чисел. Порядок элементов массива соответствует порядку элементов сырого события.
FA	KV, JSON	Массив чисел с плавающей точкой. Порядок элементов массива соответствует порядку элементов сырого события.

6. В поле **Имя** поля укажите имя поля расширенной схемы событий.

   Имя поля расширенной схемы событий имеет следующие особенности:

   - Имя должно быть уникальным в рамках экземпляра KUMA.
   - Имя чувствительно к регистру. Например, имена `Имя_поля` и `имя_поля` считаются разными именами.
   - Допустимо использовать символы латиницы, кириллицы и числа. Не допускается использование пробелов и символов " ~ ` @ # $ % ^ & * ( ) + - [ ] { } | \ | / . " < > ; ! , : ? =.
   - Если вы хотите использовать поля расширенной схемы событий для поиска источников событий, допустимо использовать только символы латиницы и числа.
   - Максимальная длина – 128 символов.

7. При необходимости в поле **Описание** укажите описание поля расширенной схемы событий.

   Рекомендуется в описании указывать назначение добавляемого поля расширенной схемы событий. В описании допустимо использовать только символы Unicode. Максимальная длина – 256 символов.

8. Нажмите на кнопку **Сохранить**.

Новое поле расширенной схемы событий будет добавлено и отобразится в начале таблицы. Будет создано событие аудита о создании поля расширенной схемы событий. Если вы включили поле, вы сможете использовать его в нормализаторах и при конфигурации ресурсов.

Изменение полей расширенной схемы событий

Пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Редактирование общих ресурсов могут изменять существующие поля расширенной схемы событий.

Чтобы изменить поле расширенной схемы событий:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Поля расширенной схемы событий**.

   Откроется окно **Поля расширенной схемы событий**.

3. Выберите название поля, которое требуется изменить.

   Откроется панель **Редактирование расширенной схемы**. В этой панели отображаются параметры выбранного поля, а также таблица **Зависимости** со списком ресурсов, макетов панели мониторинга, отчетов, пресетов и наборов полей для поиска источников событий, в которых используется это поле. Отображаются только те ресурсы, к тенантам которых у вас есть доступ. Если поле используется в тех ресурсах, к тенантам которых у вас нет доступа, эти ресурсы не будут отображаться в таблице. Ресурсы в таблице отсортированы по названию.

   Вы можете нажать на название ресурса или сущности, чтобы перейти на его страницу (кроме ресурсов панели мониторинга, пресетов и сохраненных запросов пользователей).

4. Внесите необходимые изменения в доступные параметры.

   Вы можете изменить параметры **Тип** и **Имя поля**, только если у этого поля расширенной схемы событий нет зависимостей. Параметры **Статус** и **Описание** вы можете изменить для любого поля расширенной схемы событий. Поле со статусом **Выключено** все еще будет использоваться в уже работающих конфигурациях ресурсов, пока вы не удалите его из конфигурации вручную, а также будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

   Выключить использование поля расширенной схемы событий с помощью параметра **Статус** может только пользователь с ролью Главный администратор.

5. Нажмите на кнопку **Сохранить**.

Поле расширенной схемы событий обновлено. Будет создано событие аудита об изменении поля.

Импорт и экспорт полей расширенной схемы событий

Вы можете добавить сразу несколько новых полей расширенной схемы событий, импортировав их из файла в формате JSON. Вы также можете экспортировать все существующие в KUMA поля расширенной схемы событий с информацией о них в файл, например, для передачи списка полей в другие экземпляры KUMA для поддержания работы ресурсов.

Импортировать и экспортировать поля расширенной схемы событий могут пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Редактирование общих ресурсов. Пользователи с ролью Чтение общих ресурсов могут только экспортировать поля расширенной схемы событий.

Чтобы импортировать поля расширенной схемы событий в KUMA из файла:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Поля расширенной схемы событий**.

   Откроется окно **Поля расширенной схемы событий**.

3. Нажмите на кнопку **Импортировать**.

4. В открывшемся окне выберите файл в формате JSON со списком объектов полей расширенной схемы событий.

   Пример файла JSON:

```
[
{"kind": "SA",
"name": "<fieldName1>",
"description": "<description1>",
"disabled": false},
{"kind": "N",
"name": "<fieldName2>",
"description": "<description2>",
"disabled": false},
....
{"kind": "FA",
"name": "<fieldNameX>",
"description": "<descriptionX>",
"disabled": false}
]
```

   При импорте полей из файла их имена проверяются на возможные конфликты внутри одного типа. Если в KUMA уже существует поле с таким названием и типом, такие поля из файла не будут импортированы.

Поля расширенной схемы событий будут импортированы из файла в KUMA. Будет создано событие аудита об импорте полей, а также на каждое добавляемое поле будет создано отдельное событие аудита.

Чтобы экспортировать поля расширенной схемы событий в файл:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Поля расширенной схемы событий**.

   Откроется окно **Поля расширенной схемы событий**.

3. Если вы хотите экспортировать конкретные поля расширенной схемы событий, выполните следующие действия:

   a. Установите флажки в первом столбце таблицы напротив необходимых полей.

      Вы не можете выбрать служебные поля.

   b. Нажмите на кнопку **Экспортировать выбранные** в верхней части таблицы.

4. Если вы хотите экспортировать все поля расширенной схемы событий, нажмите на кнопку **Экспортировать все** в верхней части таблицы.

Файл JSON со списком объектов полей расширенной схемы событий и информацией о них будет скачан.

Удаление полей расширенной схемы событий

Удалять поля расширенной схемы событий может только пользователь с ролью Главный администратор.

Вы можете удалить только те поля расширенной схемы событий, которые не являются служебными, у которых установлен статус **Выключено** и которые не используются в ресурсах и других объектах KUMA (нет зависимостей). Рекомендуется удалять поля расширенной схемы событий через некоторые время после того, как события, в которых использовалось поле, были гарантированно удалены из KUMA. После удаления поле не будет отображаться в подсказках событий.

Чтобы удалить поля расширенной схемы событий:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Поля расширенной схемы событий**.

   Откроется окно **Поля расширенной схемы событий**.

3. Установите флажки в первом столбце таблицы напротив одного или нескольких полей, которые вы хотите удалить.

   Вы можете выбрать все поля, установив флажок в первом столбце заголовка таблицы.

4. Нажмите на кнопку **Удалить** в верхней части таблицы.

   Кнопка **Удалить** активна, только если все выбранные поля выключены и не имеют зависимостей. Если хотя бы одно поле включено или имеет зависимость, кнопка неактивна.

   Если вы хотите удалить поле, которое используется хотя бы в одном ресурсе KUMA (имеет зависимость), но у вас нет доступа к его тенанту, кнопка **Удалить** будет активна при выборе этого поля, но при попытке удалить его отобразится ошибка.

Выбранные поля будут удалены. Будет создано событие аудита об удалении полей.

Использование полей расширенной схемы событий в нормализаторах

При использовании полей расширенной схемы событий сохраняется общее ограничение для максимального размера события обрабатываемого коллектором – 4 МБ. Информация о типах полей расширенной схемы событий приведена в таблице ниже (пункт 6 инструкции).

Использование значительного количества уникальных полей расширенной схемы событий может привести к снижению производительности системы, увеличению объема дискового пространства, необходимого для хранения событий, сложности восприятия данных.

Рекомендуется предварительно продумать и сформировать минимально необходимый набор дополнительных полей расширенной схемы событий и использовать его в нормализаторах и корреляции.

Чтобы использовать поля расширенной схемы событий:

1. Откройте существующий или создайте новый нормализатор.
2. заполнить основные параметры нормализатора;
3. нажать на кнопку **Добавить строку**;
4. в параметре **Исходные данные** указать название исходного поля в сыром событии;
5. В параметре **Поле KUMA** начните вводить имя поля расширенной схемы событий и выберите нужное поле в раскрывающемся списке.

   Поля расширенной схемы событий в раскрывающемся списке имеют имя в формате `<тип>.<имя поля>`.
6. Нажмите на кнопку **Сохранить** для сохранения нормализатора событий.

Нормализатор сохранен с выбранным полем расширенной схемы событий.

Если данные, находящиеся в полях сырого события, не соответствуют типу поля KUMA, в процессе нормализации событий значение не будет сохранено, если невозможно выполнить преобразование типов данных. Например, строка `test` не может быть помещена в числовое поле `KUMA DeviceCustomNumber1`.

С точки зрения нагрузки на сервер хранения при операциях поиска событий, подготовки отчетов и других операций с событиями в хранилище наиболее предпочтительными являются поля схемы событий KUMA, после чего идут поля расширенной схемы событий, затем поля `Extra`.

Генерация регулярных выражений с помощью KIRA

Вы можете автоматически создать одно или несколько регулярных выражений на основе примеров событий для нормализатора с методом парсинга **regexp** с помощью Kaspersky Investigation and Response Assistant. Эта функция доступна пользователям с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик.

Чтобы сгенерировать регулярные выражения:

1. Получите лицензию с AI-модулем и активируйте функциональность в KUMA.
2. Настройте интеграцию с KIRA одним из следующих способов:
   - с использованием Kaspersky Security Network (режим **KSN**);
   - с использованием стороннего LLM-провайдера (режим **Custom**).
3. Запустите создание нормализатора или откройте параметры существующего нормализатора.
4. На вкладке **Схема нормализации** в раскрывающемся списке **Метод парсинга** выберите **regexp**.
5. В поле **Примеры событий** добавьте один или несколько примеров событий, на основе которых требуется создать регулярное выражение.

   Вы можете добавить не более 10 однострочных событий.
6. Нажмите на кнопку **Сгенерировать регулярное выражение с помощью KIRA**.
7. Подтвердите отправку запроса.

   После обработки запроса откроется окно, в котором отображаются:

   - количество оставшихся токенов (если у вас настроена интеграция с KIRA с использованием KSN);
   - количество токенов, использованных при генерации;
   - сгенерированные регулярные выражения с цветовой подсветкой групп и соответствующих фрагментов примеров событий.

   Каждое сгенерированное регулярное выражение содержит в начале группу символов (?:ai)?.

   В окне с созданными выражениями вы можете отредактировать и скопировать регулярное выражение, а также применить результат генерации, нажав на кнопку **Применить**.

   > Если генерация регулярного выражения завершается ошибкой или не дает ожидаемого результата, это может означать, что используемая модель провайдера не смогла правильно определить компоненты события или сформировать регулярное выражение. В этом случае добавьте в поле **Примеры событий** несколько других похожих примеров и запустите генерацию повторно.

   После применения результата сгенерированное регулярное выражение автоматически добавляется в поле **Нормализация**. Если было сгенерировано несколько регулярных выражений, автоматически создается соответствующее количество полей для каждого выражения. Регулярные выражения добавляются в порядке их генерации, который при необходимости можно изменить, перетаскивая выражения с помощью значка ⠿.
8. После применения результата генерации регулярных выражений сохраните параметры нормализатора, нажав на кнопку **OK** и затем на кнопку **Сохранить**.

Обогащение в нормализаторе

При создании правил парсинга событий в окне параметров нормализатора на вкладке **Обогащение** вы можете настроить правила дополнения полей нормализованного события другими данными с помощью правил обогащения. Эти правила хранятся в параметрах нормализатора, в котором они были созданы.

Чтобы создать обогащение, нужно нажать на кнопку **Добавить обогащение**. Правил обогащения может быть несколько. При необходимости обогащения можно удалять с помощью кнопки ×.

Параметры, доступные в блоке параметров правила обогащения:

- **Тип источника** (обязательно) – раскрывающийся список для выбора типа обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы источников обогащения:

  - **константа**

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

    - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

    - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

  - **dictionary**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

    Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

    Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

    Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

    Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр
    - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбран тип **Событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом `Массив строк`, а целевым полем является поле с типом `Строка`, значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем `Массив строк` и целевое поле полем `Массив строк`, значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` — это название поля события, значение которого должно быть передано в скрипт.

    Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Целевое поле** (обязательно) – раскрывающийся список для выбора поля события KUMA, в которое следует поместить данные.

  Этот параметр недоступен для типа источника обогащения **таблица**.

Условия передачи данных в дополнительный нормализатор

При создании дополнительных правил парсинга событий вы можете указать условия. При выполнении этих условий события отправляются на обработку в созданное правило парсинга. Условия можно задать в окне **Дополнительный парсинг событий** на вкладке **Условия дополнительной нормализации**. В основных правилах парсинга эта вкладка отсутствует.

Доступные параметры:

- **Использовать сырое событие** – если вы хотите передавать сырое событие для дополнительной нормализации, в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**. По умолчанию указано значение **Нет**. Рекомендуется передавать сырое событие в нормализаторы типа json и xml. Если вы хотите передавать сырое событие для дополнительной нормализации на второй, третий и далее уровень вложенности, последовательно на каждом уровне вложенности в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**.

- **Поле, которое следует передать в нормализатор** – используется для указания поля события в том случае, если вы хотите отправлять на дополнительный парсинг только события с заданными в параметрах нормализатора полями.

  Если оставить это поле пустым, в дополнительный нормализатор будет передано событие целиком.

- Блок фильтров – используется для формулирования сложных условий, которым должны удовлетворять события, поступающие в нормализатор.

  С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия (см. ниже).

  С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия.

  Условия и группы можно менять местами, перетягивая их за значок ⠿, а также удалять с помощью значка ✕.

Параметры условий фильтра:

- **Левый операнд** и **Правый операнд** – используются для указания значений, которые будет обрабатывать оператор.

  В левом операнде следует указывать исходное поле событий, поступающих в нормализатор. Например, если в окне **Основной парсинг событий** настроено сопоставление eventType - DeviceEventClass, то в окне **Дополнительный парсинг событий** на вкладке **Условия дополнительной нормализации** в поле левого операнда для фильтра следует указать eventType. Данные обрабатываются только как текстовые строки.

- Операторы:

  - **=** – полное совпадение левого и правого операндов.

  - **startsWith** – левый операнд начинается с символов, указанных в правом операнде.

  - **endsWith** – левый операнд заканчивается символами, указанными в правом операнде.

  - **match** – левые операнд соответствует регулярному выражению (RE2), указанному в правом операнде.

  - **in** – левый операнд соответствует одному из значений, указанных в правом операнде.

Входящие данные можно преобразовать, нажав на кнопку 🔧. Откроется окно **Преобразование**, в котором вы можете нажать на кнопку **Добавить преобразование**, чтобы создать правила изменения исходных данных перед тем, как над ними будут совершены какие-либо действия. В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⠿, а также удалять с помощью значка ✕.

Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр

- **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

Поддерживаемые источники событий

KUMA поддерживает нормализацию событий, которые поступают от систем, перечисленных в таблице ниже. Нормализаторы для указанных систем включены в поставку.

Поддерживаемые источники событий

Название системы	Название нормализатора	Тип.	Описание нормализатора
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	Предназначен для обработки журнала событий системы 1С. Источник событий – журнал регистрации 1С.
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	Предназначен для обработки технологического журнала событий. Источник событий – технологический журнал 1С.
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ahnlab UTM	[OOTB] Ahnlab UTM	regexp	Предназначен для обработки событий от системы Ahnlab. Источник событий – системные, операционные журналы, подключения, модуль IPS.
AhnLabs MDS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Alcatel AOS-W	[OOTB] Alcatel AOS-W syslog	regexp	Предназначен для обработки части событий, поступающих от системы Alcatel AOS-W версии 6.4 по syslog.
Alcatel Network Switch	[OOTB] Alcatel Network Switch syslog	Syslog	Предназначен для обработки некоторых типов событий, полученных от сетевых коммутаторов Alcatel по syslog.
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	Предназначен для обработки событий в журналах СУБД Apache Cassandra версии 4.0.
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Atlassian Confluence	[OOTB] Atlassian Jira Confluence file	regexp	Предназначен для обработки событий систем Atlassian Jira, Atlassian Confluence (Jira версия 9.12, Confluence версия 8.5), хранящихся в файлах.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Atlassian Jira	[OOTB] Atlassian Jira Confluence file	regexp	Предназначен для обработки событий систем Atlassian Jira, Atlassian Confluence (Jira версия 9.12, Confluence версия 8.5), хранящихся в файлах.
Avanpost FAM	[OOTB] Avanpost FAM syslog	regexp	Предназначен для обработки событий системы Avanpost Federated Access Manager (FAM) версии 1.9, поступающих по syslog.
Avanpost IDM	[OOTB] Avanpost IDM syslog	regexp	Предназначен для обработки событий системы Avanpost IDM, поступающих по syslog.
Avanpost PKI	[OOTB] Avanpost PKI syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Avanpost PKI 6.0 в формате CEF по syslog.
Avaya Aura Communication Manager	[OOTB] Avaya Aura Communication Manager syslog	regexp	Предназначен для обработки части событий, поступающих от системы Avaya Aura Communication Manager версии 7.1 по syslog.
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Arbor Pravail	[OOTB] Arbor Pravail syslog	Syslog	Предназначен для обработки событий системы Arbor Pravail, поступающих по syslog.
Aruba Aruba AOS-S	[OOTB] Aruba Aruba AOS-S syslog	regexp	Предназначен для обработки некоторых типов событий, поступающих от сетевых устройств Aruba с прошивкой Aruba AOS-S версии 16.10 по syslog. Нормализатор поддерживает обработку следующих типов событий: accounting events, ACL events, ARP protect events, authentication events, console events, loop protect events.
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway syslog	regexp	Предназначен для обработки событий, поступающих от системы Barracuda Cloud Email Security Gateway по syslog.
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway syslog	Syslog	Предназначен для обработки части событий, поступающих от системы Barracuda Web Security Gateway версии 15.0 по syslog.
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BeyondTrust's BeyondInsight	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по syslog.
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	Предназначен для обработки событий от системы Symantec Endpoint Protection.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Brocade Fabric OS	[OOTB] Brocade Fabric OS syslog	Syslog	Предназначен для обработки событий Brocade Fabric OS версии 9.1, поступающих по syslog.
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	Предназначен для обработки событий, поступающих по syslog от системы Canonical LXD версии 5.18.
Checkpoint	[OOTB] Checkpoint syslog	Syslog	[OOTB] Checkpoint syslog - предназначен для обработки событий, поступающих от сетевого экрана Checkpoint версии R81 по протоколу syslog.
Cisco Access Control Server (ACS)	[OOTB] Cisco ACS syslog	regexp	Предназначен для обработки событий системы Cisco Access Control Server (ACS), поступающих по syslog.
Cisco ASA	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для некоторых событий Cisco ASA и устройств под управлением Cisco IOS, поступающих по syslog.
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	Предназначен для обработки журнала событий прокси-сервера Cisco Email Security Appliance (WSA), файл access.log.
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	Предназначен для обработки некоторых типов событий, полученных от сетевых коммутаторов Alcatel по syslog.
Cisco Firepower Threat Defense	[OOTB] Cisco ASA and IOS Syslog	Syslog	Предназначен для обработки событий для сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), поступающих по syslog.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	Предназначен для обработки событий системы Cisco Identity Services Engine (ISE), поступающих по syslog.
Cisco IOS	[OOTB] Cisco ASA and IOS Syslog	Syslog	Предназначен для некоторых событий Cisco ASA и устройств под управлением Cisco IOS, поступающих по syslog.
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	Предназначен для обработки событий, поступающих Cisco Netflow версии 5.
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	Предназначен для обработки событий, поступающих Cisco Netflow версии 9.
Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	Предназначен для обработки событий системы Cisco Prime версии 3.10, поступающих по syslog.
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cisco Unified Communications Manager	[OOTB] Cisco Unified Communications Manager	regexp	Предназначен для обработки типов событий, поступающих от системы Cisco Unified Communications Manager версии 11.5.1.
Cisco WLC	[OOTB] Cisco WLC syslog	regexp	Нормализатор для некоторых типов событий, поступающих от сетевых устройств Cisco WLC (2500 Series Wireless Controllers, 5500 Series Wireless Controllers, 8500 Series Wireless Controllers, Flex 7500 Series Wireless Controllers) по syslog.
Cisco WSA	[OOTB] Cisco WSA file, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA file. Нормализатор предназначен для обработки журнала событий прокси-сервера Cisco WSA (версии 14.2, 15.0). Нормализатор поддерживает обработку событий, сформированных с использованием шаблона: %t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr %?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%. %) %q %k %u %m [OOTB] Cisco WSA syslog. Нормализатор предназначен для обработки событий, поступающих от системы Cisco WSA (версия 15.0) по syslog

Название системы	Название нормализатора	Тип.	Описание нормализатора
Citrix NetScaler	[OOTB] Citrix NetScaler syslog	regexp	Предназначен для обработки событий, поступающих от балансировщика нагрузки Citrix NetScaler версии 13.7, Citrix ADC версии NS13.0.
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	Предназначен для обработки событий системы Codemaster Mirada, поступающих по syslog.
CollabNet Subversion Edge	[OOTB] CollabNet Subversion Edge syslog	Syslog	Предназначен для обработки событий, поступающих от системы Subversion Edge (версия 6.0.2) по syslog.
CommuniGate Pro	[OOTB] CommuniGate Pro	regexp	Предназначен для обработки событий системы CommuniGate Pro версии 6.1, передаваемых агентом KUMA по протоколу TCP.
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cribl Stream	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CrowdStrike Falcon Host	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	Предназначен для обработки событий системы CyberPeak Spektr версии 3, поступающих по syslog.
Cyberprotect Cyber Backup	[OOTB] Cyberprotect Cyber Backup SQL [OOTB] Cyberprotect Cyber Backup syslog	sql, regexp	[OOTB] Cyberprotect Cyber Backup SQL – нормализатор, предназначенный для обработки событий, полученных коннектором из базы данных системы Кибер Бэкап (версия 16.5). [OOTB] Cyberprotect Cyber Backup syslog – нормализатор, предназначенный для обработки событий, поступающих в формате CEF от системы Кибер Бэкап (версия 17.2, 17.3, 18.5) по Syslog. Пакет доступен для KUMA версии 3.2 и выше.
DeepInstinct	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Dell Network Switch	[OOTB] Dell Network Switch syslog	regexp	Предназначен для обработки некоторых типов событий, полученных от сетевых коммутаторов Dell по syslog.
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
DNS сервер BIND	[OOTB] BIND syslog [OOTB] BIND file	Syslog regexp	[OOTB] BIND syslog предназначен для обработки событий DNS-сервера BIND, поступающих по syslog. [OOTB] BIND file предназначен для обработки журналов событий DNS-сервера BIND.
Docsvision	[OOTB] Docsvision syslog	Syslog	Предназначен для обработки событий аудита, поступающих от системы Docsvision по syslog.
Dovecot	[OOTB] Dovecot syslog	Syslog	Предназначен для обработки событий почтового сервера Dovecot, поступающих по syslog. Источник событий – журналы POP3/IMAP.
Dragos Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Dr.Web Enterprise Security Suite	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий Dr.Web Enterprise Security Suite версии 13.0.1 в формате CEF.

Название системы	Название нормализатора	Тип.	Описание нормализатора
EclecticIQ Intelligence Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Eltex ESR	[OOTB] Eltex ESR syslog	Syslog	Предназначен для обработки части событий, поступающих от сетевых устройств Eltex ESR по syslog.
Eltex MES	[OOTB] Eltex MES syslog	regexp	Предназначен для обработки событий, поступающих от сетевых устройств Eltex MES (поддерживаемые модели устройств: MES14xx, MES24xx, MES3708P) по syslog.
ESET Protect	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	Нормализатор для некоторых событий аудита устройства Extreme Networks Summit Wireless Controller (модель: WM3700, версия прошивки: 5.5.5.0-018R).
Factor-TS Dionis NX	[OOTB] Factor-TS Dionis NX syslog	regexp	Предназначен для обработки некоторых событий аудита, поступающих от системы Dionis NX (версия 2.0.3) по syslog.
F5 Advanced Web Application Firewall	[OOTB] F5 Advanced Web Application Firewall syslog	regexp	Предназначен для обработки событий аудита, поступающих от системы F5 Advanced Web Application Firewall по syslog.
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий, поступающих от системы Fortinet FortiAnalyzer версии 7.0, 7.2 по syslog в формате CEF.
Fortinet FortiADC	[OOTB] FortiADC syslog KV	regexp	Предназначен для обработки типов событий, поступающих от балансировщиков нагрузки Fortinet FortiADC версии 7.1 по Syslog в формате key-value.
Fortinet FortiGate	[OOTB] Syslog-CEF	regexp	Предназначен для обработки событий, поступающих от системы Fortinet FortiGate версии 7.0, 7.2 по syslog в формате CEF.
Fortinet FortiGate	[OOTB] FortiGate syslog KV	Syslog	Предназначен для обработки событий, поступающих от сетевых экранов FortiGate (версия 7.0) по syslog. Источник событий - журналы FortiGate в формате key-value.
Fortinet Fortimail	[OOTB] Fortimail	regexp	Предназначен для обработки событий системы защиты электронной почты FortiMail. Источник событий – журналы почтовой системы Fortimail.
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiWeb	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий, поступающих от системы Fortinet FortiWeb (версии 7.6.1) в формате CEF.
FreeBSD	[OOTB] FreeBSD file	regexp	Предназначен для обработки событий операционной системы FreeBSD (версия 13.1-RELEASE), хранящихся в файле. Нормализатор поддерживает обработку файлов, полученных в результате работы утилиты praudit. Пример: praudit -xl /var/audit/AUDITFILE >> file_name.log

Название системы	Название нормализатора	Тип.	Описание нормализатора
FreeIPA.	[OOTB] FreeIPA	json	Предназначен для обработки событий, поступающих от системы FreeIPA. Источник событий– журналы службы директорий Free IPA.
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	Предназначен для обработки событий системы FreeRADIUS, поступающих по syslog. Нормализатор поддерживает события от FreeRADIUS версии 3.0.
GajShield Firewall	[OOTB] GajShield Firewall syslog	regexp	Предназначен для обработки части событий, поступающих от системы GajShield Firewall версии GAJ_OS_Bulwark_Firmware_v4.35 по syslog.
Garda Monitor	[OOTB] Garda Monitor syslog	Syslog	Предназначен для обработки событий системы Garda Monitor версии 3.4, поступающих по syslog.
Gardatech GardaDB	[OOTB] Gardatech GardaDB syslog	Syslog	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, 5.4, поступающих по syslog.
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, поступающих по syslog.
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
HAProxy	[OOTB] HAProxy syslog	Syslog	Предназначен для обработки журналов системы HAProxy. Нормализатор поддерживает события типа HTTP log, TCP log, Error log от HAProxy версии 2.8.
HashiCorp Vault	[OOTB] HashiCorp Vault json	json	Предназначен для обработки событий, поступающих от системы HashiCorp Vault версии 1.16 в формате JSON. Пакет с нормализатором доступен в KUMA 3.0 и выше.
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	Предназначен для обработки событий, поступающих от сетевых экранов Huawei Eudemon. Источник событий – журналы сетевых экранов Huawei Eudemon.
Huawei iManager 2000	[OOTB] Huawei iManager 2000 file	regexp	Нормализатор, поддерживающий обработку части событий системы Huawei iManager 2000, хранящихся в файлах \client\logs\rpc, \client\logs\deploy\ossDeployment.
Huawei USG	[OOTB] Huawei USG Basic	Syslog	Предназначен для обработки событий, поступающих от шлюзов безопасности Huawei USG по syslog.
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	Предназначен для обработки некоторых типов событий системы Huawei VRP, поступающих по syslog. Нормализатор осуществляет выборку части данных из событий. Нормализатор доступен в KUMA 3.0 и выше.
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ideco UTM	[OOTB] Ideco UTM syslog	Syslog	Предназначен для обработки событий, поступающих от Ideco UTM по syslog. Нормализатор поддерживает обработку событий Ideco UTM версии 14.7, 14.10, 17.5.
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Indeed Access Manager	[OOTB] Indeed Access Manager syslog	Syslog	Предназначен для обработки событий, поступающих от системы Indeed Access Manager по syslog.
Indeed PAM	[OOTB] Indeed PAM syslog	Syslog	Предназначен для обработки событий Indeed PAM (Privileged Access Manager) версии 2.6.
Indeed SSO	[OOTB] Indeed SSO xml	xml	Предназначен для обработки событий системы Indeed SSO (Single Sign-On). Нормализатор поддерживает работу с KUMA 2.1.3 и выше.
InfoWatch Person Monitor	[OOTB] InfoWatch Person Monitor SQL	sql	Предназначен для обработки системных событий аудита из СУБД MS SQL системы InfoWatch Person Monitor версии 10.2.
InfoWatch Traffic Monitor	[OOTB] InfoWatch Traffic Monitor SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы InfoWatch Traffic Monitor.
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Название системы	Название нормализатора	Тип.	Описание нормализатора
IPFIX	[OOTB] IPFIX	ipfix	Предназначен для обработки событий в формате IP Flow Information Export (IPFIX).
Juniper JUNOS	[OOTB] Juniper - JUNOS	regexp	Предназначен для обработки событий аудита, поступающих от сетевых устройств Juniper.
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	Предназначен для обработки алертов или событий из журнала активности Kaspersky Anti Targeted Attack.
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	Предназначен для обработки событий Kaspersky CyberTrace.
Kaspersky Endpoint Detection and Response (KEDR)	[OOTB] KEDR telemetry	json	Предназначен для обработки телеметрии Kaspersky EDR, размеченных KATA. Источник событий – kafka, EnrichedEventTopic
Kaspersky Endpoint Security для Linux	[OOTB] KESL syslog cef [OOTB] KESL json	Syslog, json	[OOTB] KESL syslog cef – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Endpoint Security для Linux (KESL) версии 12.2 в формате CEF по syslog. [OOTB] KESL json – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Endpoint Security для Linux (KESL) версии 12.5 в формате JSON.
KICS/KATA	[OOTB] KICS4Net v2.x	cef	Предназначен для обработки событий KICS/KATA версии 2.x.
KICS/KATA	[OOTB] KICS4Net v3.x	Syslog	Предназначен для обработки событий KICS/KATA версии 3.x.
KICS/KATA 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	Syslog	Предназначен для обработки событий, поступающих от системы KICS/KATA версии 4.2 по syslog.
Kaspersky KISG	[OOTB] Kaspersky KISG syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky IoT Secure Gateway (KISG) версии 3.0 по syslog.
Kaspersky NGFW	[OOTB] Kaspersky NGFW CEF	cef	Предназначен для обработки событий, поступающих от системы Kaspersky NGFW версии 1.0, 1.2 в формате CEF.
Open Single Management Platform	[OOTB] KSC	cef	Предназначен для обработки событий Open Single Management Platform в формате CEF.
Open Single Management Platform	[OOTB] KSC from SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы Open Single Management Platform.
Kaspersky Security для Linux Mail Server (KLMS)	[OOTB] KLMS syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Kaspersky Security for Linux Mail Server в формате CEF по syslog.
Kaspersky Security for MS Exchange SQL	[OOTB] Kaspersky Security for MS Exchange SQL	sql	Нормализатор для событий системы Kaspersky Security for Exchange (KSE) версия 9.0, хранящихся в базе данных.
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG syslog CEF	Syslog	Предназначен для обработки событий Kaspersky Secure Mail Gateway версии 2.0 в формате CEF по syslog.
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Kaspersky Web Traffic Security в формате CEF по syslog.
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS (KV)	Syslog	Предназначен для обработки событий Kaspersky Web Traffic Security для формата Key-Value.
Kemptechnologies LoadMaster	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Kerio Control	[OOTB] Kerio Control	Syslog	Предназначен для обработки событий сетевых экранов Kerio Control.

Название системы	Название нормализатора	Тип.	Описание нормализатора
KUMA	[OOTB] KUMA forwarding	json	Предназначен для обработки событий, перенаправленных из KUMA.
LastLine Enterprise	[OOTB] LastLine Enterprise syslog cef	Syslog	Предназначен для обработки событий, поступающих от системы LastLine Enterprise версии 7.3, 8.1, 9.1 по syslog в формате CEF.
Libvirt	[OOTB] Libvirt syslog	Syslog	Предназначен для обработки событий Libvirt версии 8.0.0, поступающих по syslog.
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Linux	[OOTB] Linux audit and iptables syslog v1	Syslog	Предназначен для обработки событий операционной системы Linux. Нормализатор не поддерживает обработку событий в формате ENRICHED.
Linux auditd	[OOTB] Linux auditd syslog for KUMA 3.2	Syslog	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, поступающих по syslog. Нормализатор поддерживает работу с событиями, обработанными коллектором KUMA версии 3.2 и выше.
Linux auditd	[OOTB] Linux auditd file for KUMA 3.2	regexp	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, хранящихся в файле. Нормализатор поддерживает работу с событиями, обработанными коллектором KUMA версии 3.2 и выше.
MariaDB	[OOTB] MariaDB Audit Plugin syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по syslog.
McAfee Endpoint DLP	[OOTB] McAfee Endpoint DLP syslog	Syslog	Предназначен для обработки событий, поступающих от системы McAfee Endpoint DLP Windows версии 11.10.200 по syslog.
Microsoft 365 (Office 365)	[OOTB] Microsoft Office 365 json	json	Нормализатор предназначен для обработки событий модуля Microsoft 365.
Microsoft Active Directory Federation Service (AD FS)	[OOTB] Microsoft Products for KUMA 3	xml	Предназначен для обработки событий Microsoft AD FS. Нормализатор [OOTB] Microsoft Products for KUMA 3 поддерживает работу с данным источником событий в KUMA 3.0.1 и выше.
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products for KUMA 3	xml	Предназначен для обработки событий Microsoft AD DS. Нормализатор [OOTB] Microsoft Products for KUMA 3 поддерживает работу с данным источником событий в KUMA 3.0.1 и выше.
Microsoft Defender	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий Microsoft Defender.
Microsoft DHCP	[OOTB] MS DHCP file	regexp	Предназначен для обработки событий от DHCP-сервера Microsoft. Источник событий – журналы DHCP сервера Windows.
Microsoft DNS	[OOTB] DNS Windows	regexp	Предназначен для обработки событий DNS сервера Microsoft. Источник событий – журналы DNS сервера Windows. Нормализатор не поддерживает обработку событий журнала отладки с включенным параметром **Details**.
Microsoft Exchange	[OOTB] Exchange CSV	csv	Предназначен для обработки журнала событий системы Microsoft Exchange. Источник событий – журналы MTA сервера Exchange.
Microsoft Hyper-V	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий Microsoft Windows. Источник событий – журналы Microsoft Hyper-V: Microsoft-Windows-Hyper-V-VMMS-Admin, Microsoft-Windows-Hyper-V-Compute-Operational, Microsoft-Windows-Hyper-V-Hypervisor-Operational, Microsoft-Windows-Hyper-V-StorageVSP-Admin, Microsoft-Windows-Hyper-V-Hypervisor-Admin, Microsoft-Windows-Hyper-V-VMMS-Operational, Microsoft-Windows-Hyper-V-Compute-Admin.
Microsoft IIS	[OOTB] IIS Log File Format	regexp	Нормализатор обрабатывает события в формате, описанном по ссылке: https://learn.microsoft.com/en-us/windows/win32/http/iis-logging. Источник событий – журналы Microsoft IIS.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Нормализатор предназначен для обработки событий операционной системы Microsoft Windows. Источник событий – события Network Policy Server.
Microsoft SCCM	[OOTB] Microsoft SCCM file	regexp	Предназначен для обработки событий системы Microsoft SCCM версии 2309. Нормализатор поддерживает обработку части событий, хранящихся в файле AdminService.log.
Microsoft SharePoint Server	[OOTB] Microsoft SharePoint Server diagnostic log file	regexp	Нормализатор поддерживает обработку части событий системы Microsoft SharePoint Server 2016, хранящихся в диагностических журналах.
Microsoft Sysmon	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Нормализатор предназначен для обработки событий модуля Microsoft Sysmon.
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки части событий из журналов Security, System, Application операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в KUMA от Kaspersky Endpoint Security для Windows 12.6 по syslog.
Microsoft-Windows-PowerShell	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий Microsoft Windows PowerShell.
Microsoft-Windows-PowerShell-Operational	[OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий журналов PowerShell-Operational операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в KUMA от Kaspersky Endpoint Security для Windows 12.6 по Syslog.
\10320287Microsoft → Windows → System log → Netlogon	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → System log → Netlogon в формате XML.

Название системы	Название нормализатора	Тип.	Описание нормализатора
\9975741Microsoft → Windows → TaskScheduler → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → TaskScheduler → Operational в формате XML.
\10320287Microsoft → Windows → WinRM → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → WinRM → Operational в формате XML.
Microsoft SQL Server	[Deprecated] [OOTB] Microsoft SQL Server xml	xml	Предназначен для обработки событий MS SQL Server версии 2008, 2012, 2014, 2016. Нормализатор поддерживает работу с KUMA 2.1.3 и выше.
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий Microsoft Windows. Источник событий – журнал Applications and Services Logs – Microsoft – Windows – TerminalServices – LocalSessionManager – Operational. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в KUMA от Kaspersky Endpoint Security для Windows 12.6 по syslog.
Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки части событий из журналов Security, System операционной системы Microsoft Windows Server. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в KUMA от Kaspersky Endpoint Security для Windows 12.6 по syslog.
Microsoft Windows XP/2003.	[OOTB] SNMP. Windows {XP/2003}	json	Предназначен для обработки событий, поступающих от рабочих станций и серверов под управлением операционных систем Microsoft Windows XP, Microsoft Windows 2003 с использованием протокола SNMP.
Microsoft WSUS	[OOTB] Microsoft WSUS file	regexp	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, 5.4, поступающих по syslog.
MikroTik	[OOTB] MikroTik syslog	regexp	Предназначен для событий, поступающих от устройств MikroTik по syslog.
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	Предназначен для обработки событий от EDR системы Minerva.
MongoDb	[OOTB] MongoDb syslog	Syslog	Предназначен для обработки части событий, поступающих от базы данных MongoDb версии 7.0 по syslog.
Multifactor Radius Server for Windows	[OOTB] Multifactor Radius Server for Windows syslog	Syslog	Предназначен для обработки событий, поступающих от системы Multifactor Radius Server версии 1.0.2 для Microsoft Windows по протоколу syslog.
MySQL 5.7.	[OOTB] MariaDB Audit Plugin syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по syslog.
NetApp ONTAP (AFF, FAM)	[OOTB] NetApp syslog, [OOTB] NetApp file	regexp	[OOTB] NetApp syslog – предназначен для обработки событий системы NetApp (версия – ONTAP 9.12), поступающих по syslog. [OOTB] NetApp file - предназначен для обработки событий системы NetApp (версия - ONTAP 9.12), хранящихся в файле.

Название системы	Название нормализатора	Тип.	Описание нормализатора
NetApp SnapCenter	[OOTB] NetApp SnapCenter file	regexp	Предназначен для обработки части событий системы NetApp SnapCenter (версия SnapCenter Server 5.0). Нормализатор поддерживает обработку части событий из файла C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\napManagerWeb.*.log. Типы поддерживаемых событий в формате xml из файла SnapManagerWeb.*.log: SmDiscoverPluginRequest, SmDiscoverPluginResponse, SmGetDomainsResponse, SmGetHostPluginStatusRequest, SmGetHostPluginStatusResponse, SmGetHostRequest, SmGetHostResponse, SmRequest. Нормализатор поддерживает обработку части событий из файла C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\audit.log.
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NetScout Systems nGenius Performance Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Nextcloud	[OOTB] Nextcloud syslog	Syslog	Предназначен для событий Nextcloud версии 26.0.4, поступающих по syslog. Нормализатор не сохраняет информацию из поля Trace.
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Nginx	[OOTB] Nginx regexp	regexp	Предназначен для обработки событий журнала веб-сервера Nginx.
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
OpenLDAP	[OOTB] OpenLDAP	regexp	Предназначен для построчной обработки части событий системы OpenLDAP версия 2.5, файл auditlog.ldif.
Open VPN	[OOTB] OpenVPN file	regexp	Предназначен для обработки журнала системы OpenVPN.
Oracle	[OOTB] Oracle Audit Trail	sql	Предназначен для обработки событий аудита БД, полученных коннектором непосредственно из базы данных Oracle.
OrionSoft Termit	[OOTB] OrionSoft Termit syslog	Syslog	Предназначен для обработки событий, поступающих от системы OrionSoft Termit версии 2.2, 2.3, 2.4 по Syslog.
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	Предназначен для обработки событий системы виртуализации Orion soft zVirt версии 3.1.
PagerDuty	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Networks NGFW	[OOTB] PA-NGFW (Syslog-CSV)	Syslog	Предназначен для обработки событий от сетевых экранов Palo Alto Networks, поступающих по syslog в формате CSV.
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Parsec ParsecNet	[OOTB] Parsec ParsecNet	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы Parsec ParsecNet версии 3.
Passwork	[OOTB] Passwork syslog	Syslog	Предназначен для обработки событий, поступающих от системы Passwork версии 050219 по syslog.
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	Предназначен для обработки событий от системы PT Industrial Security Incident Manager.
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PT NAD json	json	Предназначен для обработки событий, поступающий от PT NAD в формате json. Нормализатор поддерживает обработку событий PT NAD версий 11.1, 11.0.
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	Предназначен для обработки событий системы PT Sandbox.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF	Syslog	Предназначен для обработки событий, поступающих от системы PTsecurity (Web Application Firewall).
Postfix	[OOTB] Postfix syslog	regexp	Пакет [OOTB] Postfix содержит набор ресурсов для обработки событий Postfix версии 3.6. Поддерживается обработка syslog-событий, поступающих по протоколу TCP. Пакет доступен для KUMA версии 3.0 и выше.
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit syslog	Syslog	Предназначен для обработки событий плагина аудита pgAudit для базы данных PostgreSQL, поступающих по syslog.
PowerDNS	[OOTB] PowerDNS syslog	Syslog	Предназначен для обработки событий PowerDNS Authoritative Server версии 4.5, поступающих по syslog.
Proftpd	[OOTB] Proftpd syslog	regexp	Предназначен для обработки событий, поступающих от Proftpd 1.3.8c по syslog.
Proofpoint Insider Threat Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Proxmox	[OOTB] Proxmox file	regexp	Предназначен для событий системы Proxmox версии 7.2-3, хранящихся в файле. Нормализатор поддерживает обработку событий в журналах access и pveam.
PT NAD	[OOTB] PT NAD json	json	Предназначен для обработки событий, поступающий от PT NAD в формате json. Нормализатор поддерживает обработку событий PT NAD версий 11.1, 11.0.
QEMU - журналы гипервизора	[OOTB] QEMU - Hypervisor file	regexp	Предназначен для обработки событий гипервизора QEMU, хранящихся в файле. Поддерживаются версии QEMU 6.2.0, Libvirt 8.0.0.
QEMU - журналы виртуальных машин	[OOTB] QEMU - Virtual Machine file	regexp	Предназначен для обработки событий из журналов виртуальных машин гипервизора QEMU версии 6.2.0, хранящихся в файле.
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по Syslog.
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider file	regexp	Предназначен для обработки событий системы Reak Soft Blitz Identity Provider версии 5.16, хранящихся в файле.
RedCheck Desktop	[OOTB] RedCheck Desktop file	regexp	Предназначен для обработки журналов системы RedCheck Desktop 2.6, хранящихся в файле.
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	Предназначен для обработки журналов системы RedCheck Web 2.6, хранящихся в файлах.
РЕД СОФТ РЕД АДМ	[OOTB] RED SOFT RED ADM syslog	regexp	Предназначен для обработки событий, поступающих от системы РЕД АДМ (версия РЕД АДМ: Промышленная редакция 1.1) по syslog. Нормализатор поддерживает обработку событий: - подсистемы управления; - контроллера.
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	Предназначен для обработки событий, поступающих от сетевого экрана pfSense, поступающих по syslog.
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	Предназначен для обработки событий, поступающих от сетевого экрана pfSense. Syslog-заголовок этих событий не содержит имени устройства.

Название системы	Название нормализатора	Тип.	Описание нормализатора
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
SecurityCode Continent 4	[OOTB] SecurityCode Continent 4 syslog	regexp	Предназначен для обработки событий системы SecurityCode Continent версии 4, поступающих по syslog.
Sendmail	[OOTB] Sendmail syslog	Syslog	Предназначен для обработки событий Sendmail версии 8.15.2, поступающих по syslog.
SentinelOne	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Skype for Business	[OOTB] Microsoft Products for KUMA 3	xml	Предназначен для обработки части событий из журнала системы Skype for Business, журнал Lync Server.
Snort	[OOTB] Snort 3 json file	json	Предназначен для обработки событий Snort версии 3 в формате JSON.
Sophos Central	[OOTB] Sophos Central syslog	Syslog	Предназначен для обработки части событий, поступающих от системы Sophos Central версии 1.2 по syslog в формате CEF от интеграционного скрипта Sophos-Central-SIEM-Integration.
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall	Syslog	Предназначен для обработки событий, поступающих по syslog от сетевого экрана Sonicwall TZ.
Solar WebProxy	[OOTB] Solar WebProxy syslog	regexp	Предназначен для обработки событий, поступающих от Solar WebProxy версии 4.2 в формате siem-log по syslog.
SolarWinds DameWare MRC	[OOTB] SolarWinds DameWare MRC xml	xml	Нормализатор, поддерживающий обработку части событий системы DameWare Mini Remote Control (MRC) версия 7.5, хранящихся в журнале Application операционной системы Windows. Нормализатор обрабатывает события, создаваемые провайдером dwmrcs.
Sophos Firewall	[OOTB] Sophos Firewall syslog	regexp	Предназначен для обработки событий, поступающих от Sophos Firewall версии 20 по syslog.
Sophos XG	[OOTB] Sophos XG	regexp	Предназначен для обработки событий от сетевого экрана Sophos XG.
Squid	[OOTB] Squid access syslog	Syslog	Предназначен для обработки событий прокси-сервера Squid, поступающих по протоколу syslog.
Squid	[OOTB] Squid access.log file	regexp	Предназначен для обработки событий журнала Squid прокси-сервера Squid. Источник событий – журналы access.log
Staffcop Enterprise	[OOTB] Staffcop Enterprise syslog CEF	regexp	Предназначен для обработки событий, поступающих от Staffcop Enterprise версии 5.4, 5.5 в формате CEF по syslog.
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	Предназначен для обработки событий от устройств S-Terra VPN Gate.
Stormshield firewall	[OOTB] Stormshield firewall syslog	Syslog	Предназначен для обработки событий, поступающих от системы Stormshield firewall версии 4.8 и 5.0 в формате key-value по протоколу Syslog.
Suricata	[OOTB] Suricata json file	json	Пакет содержит нормализатор для событий Suricata версии 7.0.1, хранящихся в файле в формате JSON. Нормализатор поддерживает обработку следующих типов событий: flow, anomaly, alert, dns, http, ssl, tls, ftp, ftp_data, ftp, smb, rdp, pgsql, modbus, quic, dhcp, bittorrent_dht, rfb.
ThreatConnect Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Tionix Cloud Platform	[OOTB] Tionix Cloud Platform syslog	Syslog	Предназначен для обработки событий системы Tionix Cloud Platform версии 2.9, поступающих по syslog. Нормализатор осуществляет выборку части данных из событий. Нормализатор доступен в KUMA 3.0 и выше.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Tionix VDI	[OOTB] Tionix VDI file	regexp	Нормализатор, поддерживающий обработку части событий системы Tionix VDI (версия 2.8), хранящихся в файле tionix_lntmov.log.
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Control Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Unbound	[OOTB] Unbound syslog	Syslog	Предназначен для обработки событий, поступающих по syslog от DNS-сервера Unbound.
UserGate	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы UserGate по syslog.
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Veriato 360	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
ViPNet TIAS	[OOTB] Vipnet TIAS syslog	Syslog	Предназначен для обработки событий системы ViPNet TIAS версии 3.8, поступающих по syslog.
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	Предназначен для обработки событий VMware ESXi (поддержка ограниченного количества событий от ESXi с версиями 5.5, 6.0, 6.5, 7.0), поступающих по syslog.
VMWare Horizon	[OOTB] VMWare Horizon - Syslog	Syslog	Предназначен для обработки событий, поступающих от системы VMWare Horizon версии 2106 по syslog.
VMwareCarbon Black EDR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Vmware vCenter	[OOTB] VMware vCenter API	xml	Предназначен для обработки событий VMware vCenter версии 7, получаемых по API.
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Vsftpd	[OOTB] Vsftpd syslog	regexp	Предназначен для обработки событий, поступающих от системы Vsftpd версии 3.0.5 по syslog.
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	Предназначен для событий, поступающих от системы Wallix AdminBastion по syslog.
WatchGuard - Firebox	[OOTB] WatchGuard Firebox	Syslog	Предназначен для обработки событий сетевых экранов WatchGuard Firebox, поступающих по syslog.
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Winchill Fracas	[OOTB] PTC Winchill Fracas	regexp	Предназначен для обработки событий системы регистрации сбоев Winchill Fracas.
Yandex Browser корпоративный	[OOTB] Yandex Browser	json	Предназначен для обработки событий, поступающих от корпоративной версии Яндекс Браузера версии 23 или 24.4.
Yandex Cloud	[OOTB] Yandex Cloud	regexp	Предназначен для обработки части событий аудита системы Yandex Cloud. Нормализатор поддерживает обработку событий аудитного журнала уровня конфигурации: IAM (Yandex Identity and Access Management), Compute (Yandex Compute Cloud), Network (Yandex Virtual Private Cloud), Storage (Yandex Object Storage), Resourcemanager (Yandex Resource Manager).

Название системы	Название нормализатора	Тип.	Описание нормализатора
Zabbix	[OOTB] Zabbix SQL	sql	Предназначен для обработки событий Zabbix версии 6.4.
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	Предназначен для обработки событий системы Zecurion DLP версии 12.0, поступающих по syslog
ZEEK IDS	[OOTB] ZEEK IDS json file	json	Предназначен для обработки журналов системы ZEEK IDS в формате JSON. Нормализатор поддерживает события от ZEEK IDS версии 1.8.
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
АйТи Бастион – СКДПУ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы АйТи Бастион - СКДПУ по syslog.
А-реал Интернет Контроль Сервер (ИКС)	[OOTB] A-real IKS syslog	regexp	Предназначен для обработки событий системы А-реал Интернет Контроль Сервер (ИКС), поступающих по syslog. Нормализатор поддерживает события от A-real IKS версии 7.0 и выше.
Бизнес Решения – Compass	[OOTB] Biznes Resheniya Compass	regexp	Предназначен для обработки типов событий аудита системы Бизнес Решения – Compass версии 6.7.7 и 6.7.8, поступающих из Kafka.
Веб-сервер Apache	[OOTB] Apache HTTP Server file	regexp	Предназначен для обработки событий Apache HTTP Server версии 2.4, хранящихся в файле. Нормализатор поддерживает обработку событий журнала Application в форматах Common или Combined Log, и журнала Error. Ожидаемый формат журнала Error: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Веб-сервер Apache	[OOTB] Apache HTTP Server syslog	Syslog	Предназначен для обработки событий системы Apache HTTP Server, поступающих по syslog. Нормализатор поддерживает обработку событий Apache HTTP Server версии 2.4 журнала Access в формате Common или Combined Log, и журнала Error. Ожидаемый формат журнала Error: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Веб-сервер Lighttpd	[OOTB] Lighttpd syslog	Syslog	Предназначен для обработки событий Access системы Lighttpd, поступающих по syslog. Нормализатор поддерживает обработку событий Lighttpd версии 1.4. Ожидаемый формат событий журнала Access: `$remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"`
ИВК Кольчуга-К	[OOTB] Kolchuga-K Syslog	Syslog	Предназначен для обработки событий, поступающих от системы ИВК Кольчуга-К, версии ЛКНВ.466217.002 по syslog.
ИнфоТеКС ViPNet IDS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы ИнфоТеКС ViPNet IDS по syslog.
ИнфоТеКС ViPNet Coordinator	[OOTB] VipNet Coordinator syslog	Syslog	Предназначен для обработки событий от системы ViPNet Coordinator, поступающих по syslog.
Код безопасности - Континент	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	Предназначен для обработки журнала событий устройств Континент IPS/IDS.
Код безопасности - Континент	[OOTB] Continent SQL	sql	Предназначен для получения событий системы Континент из базы данных.
Код Безопасности SecretNet 7	[OOTB] SecretNet SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы SecretNet.
Конфидент – Единый центр управления Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Предназначен для обработки событий, поступающих от системы Единый центр управления (ЕЦУ) Dallas Lock, версия 4.0 в формате CEF.
КриптоПро Ngate	[OOTB] Ngate syslog	Syslog	Предназначен для обработки событий, поступающих от системы КриптоПро Ngate по syslog.

Название системы	Название нормализатора	Тип.	Описание нормализатора
Маршрутизаторы H3C (Huawei-3Com)	[OOTB] H3C Routers syslog	regexp	Нормализатор для некоторых типов событий, поступающих от сетевых устройств H3C (Huawei-3Com) SR6600 (прошивка Comware 7) по syslog. Нормализатор поддерживает стандартный формат событий (RFC 3164-compliant format).
НТ Мониторинг и аналитика	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы НТ Мониторинг и аналитика по syslog.
Прокси-сервер BlueCoat	[OOTB] BlueCoat Proxy v0.2	regexp	Предназначен для обработки событий прокси-сервера BlueCoat. Источник событий – журнал событий прокси-сервера BlueCoat.
СКДПУ НТ Шлюз доступа	[OOTB] Bastion SKDPU-GW	Syslog	Предназначен для обработки событий системы СКДПУ НТ Шлюз доступа, поступающих по syslog.
Солар Дозор	[OOTB] Solar Dozor syslog	Syslog	Предназначен для обработки событий, поступающих от системы Солар Дозор версии 7.9 по syslog. Нормализатор поддерживает обработку событий в пользовательском формате и не поддерживает обработку событий в формате CEF.
-	[OOTB] Syslog header	Syslog	Предназначен для обработки событий, поступающих по syslog. Нормализатор выполняет парсинг Syslog-заголовка события, поле message события не затрагивается. В случае необходимости вы можете выполнить парсинг поля message другими нормализаторами.

Правила агрегации

Правила агрегации позволяют объединить однотипные повторяющиеся события и заменить их одним общим событием. В правилах агрегации поддерживается работа с полями стандартной схемы событий KUMA и с полями расширенной схемы событий. Таким образом можно уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор, снизить нагрузку на службы, сэкономить место для хранения данных и сэкономить лицензионную квоту (EPS). Агрегационное событие создается по достижении порога по времени или порога по числу событий, смотря что произойдет раньше.

Для правил агрегации можно настроить фильтр и применять его только к событиям, которые соответствуют заданным условиям.

Можно настроить правила агрегации в разделе **Мониторинг** → **Ресурсы** → **Правила агрегации**, а затем выбрать созданное правило агрегации в раскрывающемся списке в параметрах коллектора. Также можно настроить правила агрегации прямо в настройках коллектора.

Доступные параметры правил агрегации

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Предел событий	Ограничение по количеству событий. После накопления заданного количества событий с идентичными полями коллектор создает агрегационное событие и начинает накопление событий для следующего агрегированного события. По умолчанию указано значение `100`.
Время ожидания событий	Обязательный параметр. Ограничение по времени в секундах. По истечении указанного срока накопление базовых событий прекращается, коллектор создает агрегированное событие и начинает получать события для следующего агрегированного события. По умолчанию указано значение `60`.
Описание	Описание ресурса: до 4000 символов Юникода.
Группирующие поля	Обязательный параметр. В раскрывающемся списке перечислены поля нормализованных событий, значения которых должны совпадать. Например, для сетевых событий это могут быть SourceAddress, DestinationAddress, DestinationPort. В итоговом агрегационном событии эти поля будут заполнены значениями базовых событий.

Параметр	Описание
Уникальные поля	В раскрывающемся списке перечислены поля, спектр значений которых нужно сохранить в агрегированном событии. Например, если поле DestinationPort указать не в **Группирующие поля**, а в **Уникальные поля**, то агрегированное событие объединит базовые события подключения к разным портам, а поле DestinationPort агрегированного события будет содержать список всех портов, к которым выполнялись подключения.
Поля суммы	В раскрывающемся списке можно выбрать поля, значения которых при агрегации будут просуммированы и записаны в одноименные поля агрегированного события.

Параметр	Описание
Фильтр	Блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** фильтр. Не используйте в правилах агрегации фильтры с операндом **TI** или операторами **TIDetect**, **inActiveDirectoryGroup** и **hasVulnerability**. Поля Active Directory, для которых используется оператор **inActiveDirectoryGroup,** появляются на этапе обогащения, то есть после выполнения правил агрегации. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

Параметр	Описание
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде. d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила агрегации и используется для привязки правила к коллектору.

Для привязки правила агрегации к коллектору, нажмите на кнопку **Привязать к сервису** → **Привязать к коллектору**. В открывшемся окне выберите один или несколько коллекторов и нажмите **OK**. Правило агрегации будет привязано к выбранным коллекторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете отвязать правило агрегации от службы. Для этого нужно установить флажок рядом с нужным коллектором, нажать **Удалить** и подтвердить удаление привязки к службе.

Предустановленные правила агрегации

В поставку OSMP включены перечисленные в таблице ниже правила агрегации.

Название правила агрегации	Описание
[OOTB] Netflow 9	Правило сработает при достижении 100 событий или по истечении 10 секунд. Агрегация событий выполняется по полям: • DestinationAddress • DestinationPort • SourceAddress • TransportProtocol • DeviceVendor • DeviceProduct Поля DeviceCustomString1 и BytesIn суммируются.

Правила обогащения

Обогащение событий – это дополнение событий информацией, которая может быть использована для выявления инцидента и при проведении расследования.

Правила обогащения позволяют добавлять в поля события дополнительную информацию путем преобразования данных, уже размещенных в полях, или с помощью запроса данных из внешних систем. Например, в событии есть имя учетной записи пользователя. С помощью правила обогащения вы можете добавить сведения об отделе, должности и руководителе этого пользователя в поля события.

Правила обогащения можно использовать в следующих сервисах и функциях KUMA:

- Коллектор.
- Коррелятор.
- Нормализатор.

Доступные параметры правил обогащения перечислены в таблице ниже.

Вкладка Основные параметры

Параметр	Описание

Тип источника	Обязательный параметр. Раскрывающийся список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры: • **константа** Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения: • В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено. • В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные. Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа. Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива. • **dictionary** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря. Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV. Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c']. Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|". Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode. • **table** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря. Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные: • В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря. • В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных. Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕. • **событие** Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения: • В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные. • В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле. • В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение. **Доступные преобразования** Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **entropy** используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа float. Результатом преобразования является число. Вычисление информационной энтропии позволяет обнаруживать DNS-туннели или скомпрометированные пароли, например, когда пользователь вводит пароль вместо учетной записи и этот пароль регистрируется в виде обычного текста.
- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле Символы. Это поле появляется при выборе данного типа преобразования. Например, если для значения Microsoft-Windows-Sysmon выполнить преобразование trim со значением Micromon, то получается значение soft-Windows-Sys.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле Константа. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле Константа. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

    Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

  Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

  Параметры этого типа обогащения описаны в таблице ниже.

  Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то KUMA возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро KUMA.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

  Доступные параметры:

  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
  - **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.
  - **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

    Доступные типы индикаторов CyberTrace:

    - **ip**
    - **url**
    - **hash**

    В таблице сопоставления требуется указать как минимум одну строку. Нажав на кнопку **Добавить строку**, можно добавить строку, а на кнопку ✕ – удалить.

- **cybertrace-http**

Этот тип обогащения используется для добавления в поля события сведений с помощью REST API из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение 30.
- **Ключевые поля** (обязательно) – это список полей событий, используемых для обогащения событий данными из CyberTrace.
- **Максимальное количество событий в очереди обогащения** – максимальное количество событий, хранящихся в очереди обогащения для повторной отправки. По умолчанию указано значение 1000000000. При достижении 1 000 000 событий, полученных с сервера CyberTrace, обогащение событий прекращается до тех пор, пока количество полученных событий станет меньше 500 000.

> Когда значение метрики Queue достигает 1 000 000 полученных событий, обогащение событий прекращается и события записываются в Хранилище необогащенными до тех пор, пока количество событий в очереди не станет меньше 500 000.

- **часовой пояс**

Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере службы, использующей обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлена служба (коллектор или коррелятор), обрабатывающая событие. При изменении времени сервера службу необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- **геоданные;**

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

   С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. Можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события, нажав эту кнопку.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

	С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ❌. • В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**. • В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных. Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Отладка	Переключатель, с помощью которого можно включить логирование операций сервиса. По умолчанию логирование выключено.
Описание	Описание ресурса: до 4000 символов Юникода.

Фильтр	Блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила обогащения и используется для привязки правила к сервисам – корреляторам и коллекторам.

Для привязки правила обогащения к коллектору и/или коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к <название сервиса>**. В открывшемся окне выберите один или несколько корреляторов или коллекторов и нажмите **OK**. Правило обогащения будет привязано к выбранным сервисам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь правила обогащения с сервисом. Для этого установите флажок рядом с коррелятором или сборщиком, нажмите на кнопку **Удалить** и подтвердите отмену привязки к сервису.

Предустановленные правила обогащения

В поставку OSMP включены перечисленные в таблице ниже правила обогащения.

Предустановленные правила обогащения

Название правила обогащения	Описание
[OOTB] KATA alert	Используется для обогащения событий, поступивших от KATA в виде гиперссылки на алерт. Гиперссылка размещается в поле DeviceExternalId.

Правила корреляции

Правила корреляции используются для распознавания определенных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания: например, создание корреляционных событий или алертов, взаимодействие с активным листом.

Правила корреляции можно использовать в следующих сервисах и функциях KUMA:

- Коррелятор.
- Правило уведомления.
- Связи правил сегментации.
- Ретроспективная проверка.

Доступные параметры правила корреляции зависят от выбранного типа. Типы правил корреляции:

- standard – используется для поиска корреляций между несколькими событиями. Правила этого типа могут создавать корреляционные события.

  Этот тип правил используется для определения сложных закономерностей в последовательности событий. Для более простых комбинаций следует использовать другие типы правил корреляции, которые требуют меньше ресурсов.

- simple – используется для создания корреляционных событий при обнаружении определенного события.

- operational – используется для операций с активными листами и контекстными таблицами. Этот тип правил не может создавать корреляционные события.

- periodical – используется для выявления аномальной активности пользователей на основе накопленных данных, которые анализируются с определенной периодичностью. Аномалии фиксируются при превышении порогов двух метрик: относительного показателя (**Relative Score**) и стандартизированного отклонения (**Z-Score**).

  Этот тип правил доступен только при использовании коррелятора correlator-ng. Создать правило в Консоли OSMP невозможно.

  При изменении конфигурации коррелятора correlator-ng может потребоваться удаление директорий correlation/ и containers/. Удаление этих директорий приводит к потере всех накопленных данных коррелятора, включая статистику, контейнеры правил корреляции, активные листы и контекстные таблицы.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если правило корреляции используется в корреляторе и по нему был создан алерт, то при изменении правила корреляции существующий алерт не будет изменен, даже если перезапустить сервис коррелятора. Например, если у правила корреляции было изменено название, название алерта останется прежним. Если существующий алерт закрыть, то новый алерт будет создан уже с учетом изменений правила корреляции.

Правила корреляции типа standard

Правила корреляции типа **standard** используются для определения сложных закономерностей в обрабатываемых событиях.

Поиск закономерностей происходит с помощью контейнеров

Контейнеры правила корреляции – это временные хранилища данных, которые используются ресурсами правила корреляции при определении необходимости создания корреляционных событий. Эти контейнеры выполняет следующие функции:

- Группируют события, которые были отобраны фильтрами в группе настроек **Селекторы** ресурса правила корреляции. События группируются по полям, которые указываются пользователем в поле **Группирующие поля**.

- Определяют момент, когда должно сработать правило корреляции, меняя соответствующим образом события, сгруппированные в контейнере.

- Выполняют действия, указанные в группе настроек **Действия**.
- Создают корреляционные события.

Доступные состояния контейнера:

- `Пусто` – в контейнере нет событий. Это может произойти только в момент своего создания при срабатывании правила корреляции.
- `Частичное совпадение` – в контейнере есть некоторые из ожидаемых событий (события восстановления не учитываются).
- `Полное совпадение` – в корзине есть все ожидаемые события (события восстановления не учитываются). При достижении этого состояния:
  - Срабатывает правило корреляции
  - События удаляются из контейнера
  - Счетчик срабатываний контейнера обновляется
  - Контейнера переводится в состояние `Пусто`
- `Ложное совпадение` – такое состояние контейнера возможно в следующих случаях:
  - когда было достигнуто состояние `Полное совпадение`, но объединяющий фильтр возвратил значение false.
  - когда при установленном флажке **Обнуление** были получены события восстановления.

  Когда это условие достигается, правило корреляции не срабатывает. События удаляются из контейнера, счетчик срабатываний обновляется, контейнер переводится в состояния `Пусто`.

Окно правила корреляции содержит следующие вкладки:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правил.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа правил.
- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Версия ресурса в репозитории "Лаборатории Касперского"** – номер версии ресурса. Это поле невозможно изменить. Поле доступно только для ресурсов, предоставляемых "Лабораторией Касперского", и используется для управления обновлениями ресурсов.

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.

- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **standard**, если хотите создать правило корреляции типа standard.

- **Группирующие поля** (обязательно) – поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей используется в качестве ключа контейнера. Если срабатывает селектор (см. ниже), отобранные поля копируются в корреляционное событие.

  Если в разных селекторах корреляционного правила используются поля, которые имеют разные значения в событиях, эти поля не нужно указывать в разделе **Группирующие поля**.

- **Уникальные поля** – поля событий, которые должны быть отправлены в контейнер. Если задан этот параметр, в контейнер будут отправляться только уникальные поля. Хеш-код значений отобранных полей используется в качестве ключа контейнера.

  Вы можете использовать локальные переменные в разделах **Группирующие поля** и **Уникальные поля**. Для обращения к переменной необходимо перед ее именем указать символ "$".
  Для ознакомления с примерами использования локальных переменных в этих разделах используйте правило, поставляемое с KUMA: R403_Обращение на вредоносные ресурсы с устройства с выключенной защитой или устаревшей антивирусной базой.

- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Время жизни контейнера, сек.** (обязательно) – время жизни контейнера в секундах. Значение по умолчанию – 86 400 секунд (24 часа). Этот таймер запускается при создании контейнера (когда он получает первое событие). Время жизни не обновляется, и когда оно истекает, срабатывает триггер **По истечении времени жизни контейнера** из группы настроек **Действия**, а контейнер удаляется. Триггеры **На каждом срабатывании правила** и **На последующих срабатываниях правила** могут срабатывать более одного раза в течение времени жизни контейнера.

- **Политика хранения базовых событий** – этот раскрывающийся список используется, чтобы определить, какие базовые события должны быть сохранены в корреляционном событии:
  - **first** (значение по умолчанию) – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события.
  - **last** – поместить в корреляционное событие последнее базовое событие из коллекции событий, инициировавшей создание корреляционного события.
  - **all** – поместить в корреляционное событие все базовые события из коллекции событий, инициировавшей создание корреляционного события.
- **Приоритет** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию – **Низкий**.
- **Сортировать по** – в этом раскрывающемся списке можно выбрать поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, если, например, вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.
- **Описание** – описание ресурса. До 4000 символов Юникода.

Вкладка **Селекторы**

В правиле типа **standard** может быть несколько селекторов. Селекторы можно добавлять с помощью кнопки **Добавить селектор** и удалять с помощью кнопки **Удалить селектор**. Вы можете перемещать селекторы с помощью кнопки ⣿.

Для каждого селектора доступны две вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит следующие параметры:

- **Название** (обязательно) – уникальное имя группы событий, удовлетворяющих условиям селектора. Имя должно содержать от 1 до 128 символов Юникода.
- **Порог срабатывания селектора (количество событий)** (обязательно) – количество событий, которое необходимо получить для срабатывания селектора. По умолчанию указано значение 1.
- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр.

  Создание фильтра в ресурсах

  Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

   Операторы фильтров

   - **=** – левый операнд равен правому операнду.
   - **<** – левый операнд меньше правого операнда.
   - **<=** – левый операнд меньше или равен правому операнду.
   - **>** – левый операнд больше правого операнда.
   - **>=** – левый операнд больше или равен правому операнду.
   - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
   - **contains** – левый операнд содержит значения правого операнда.
   - **startsWith** – левый операнд начинается с одного из значений правого операнда.
   - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
   - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
   - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

     Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

     Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.

- Левый операнд – **поле события**.

- В поле события вы можете указать одно из следующих значений:

  - Поле **Extra**.

  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.

  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.

- Оператор – =.

- Правый операнд – **константа**.

- Значение – значение, по которому требуется фильтровать события.

  Последовательность условий, заданных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Рекомендуется на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.

  Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.

  Фильтр селектора 1:

  Условие 1. DeviceProduct = Microsoft Windows

  Условие 2. DeviceEventClassID = 4624

  Фильтр селектора 2:

  Условие 1. DeviceEventClassID = 4624

  Условие 2. DeviceProduct = Microsoft Windows

  Последовательность условий, заданная в Фильтре селектора 2, более предпочтительна, поскольку оказывает меньшую нагрузку на систему.

- **Обнуление** – этот флажок должен быть установлен, если правило корреляции НЕ должно срабатывать при получении селектором определенного количества событий. По умолчанию флажок снят.

Выбрав вкладку **Локальные переменные**, с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

В селекторе корреляционного правила могут быть использованы регулярные выражения, соответствующие стандарту RE2.

Применение регулярных выражений в правилах корреляции создает большую нагрузку в сравнении с другими операциями. Поэтому при разработке правил корреляции рекомендуется ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Для использования регулярного выражения необходимо применить оператор сравнения `match`. Регулярное выражение должно быть размещено в константе. Применение capture-групп в регулярных выражениях не обязательно. Для срабатывания корреляционного правила текст поля, сопоставляемый с regexp, должен полностью совпасть с регулярным выражением.

Для ознакомления с синтаксисом и примерами корреляционных правил, в селекторах которых есть регулярные выражения, используйте следующие правила, поставляемые с KUMA:

- R105_04_Подозрительные PowerShell-команды. Подозрение на обфускацию.
- R333_Подозрительное создание файлов в директории автозапуска.

Вкладка **Действия**

В правиле типа **standard** может быть несколько триггеров.

- **На первом срабатывании правила** – этот триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.
- **На последующих срабатываниях правила** – этот триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания селектора.
- **На каждом срабатывании правила** – этот триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.
- **По истечении времени жизни контейнера** – этот триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором с установленным флажком **Обнуление**. То есть триггер срабатывает, если в течение заданного времени ситуация, обнаруженная правилом корреляции, не разрешается.

Каждый триггер представлен в виде группы настроек со следующими доступными параметрами:

- **В дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения.
- **В коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться цепочкой правил текущего коррелятора. Это позволяет достичь иерархической корреляции.

  Если установлены флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции сначала отправляется на постобработку, а затем в селекторы текущего правила корреляции.
- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции. Если вы не хотите создавать алерт при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Не создавать алерт**. Если вы установите только флажок **Не создавать алерт**, событие корреляции не сохраняется в хранилище.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения. Эти правила обогащения хранятся в правиле корреляции, в котором они были созданы. Можно создать несколько правил обогащения. Вы можете добавлять или удалять правила обогащения с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - **константа**

      Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

      - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

      - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

    - **dictionary**

      Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

      Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

      Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

      Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

      Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

      Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.

  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.

  - Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр

    - **upper** – используется для перевода всех символов значения в верхний регистр

    - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

    - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.
- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбран тип **Событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом `Массив строк`, а целевым полем является поле с типом `Строка`, значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем `Массив строк` и целевое поле полем `Массив строк`, значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` — это название поля события, значение которого должно быть передано в скрипт.

    Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Отладка** – с помощью этого переключателя можно включить логирование операций сервиса.
- **Описание** – описание ресурса. До 4000 символов Юникода.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько. Вы можете добавлять или удалять правила категоризации с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию активу.
    - **Удалить** – отвязать актив от категории.
  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
  - **Идентификатор категории** – в раскрывающемся списке отображается дерево категорий и вы можете выбрать категорию, над которой будет совершена операция. Список раскрывается, если нажать на строку.
- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

  Доступные параметры:
  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

- **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.

- **Удалить** – удалить запись из активного листа.

- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

  - Левое поле используется для указания поля активного листа.

    Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.

  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

  - Группа параметров Обновление контекстных таблиц – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок **Добавить действие с контекстной таблицей** и **Удалить действие с контекстной таблицей** можно добавлять и удалять операции с контекстными таблицами.

  - Доступные параметры:

  - Название (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.

  - Операция (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.

  - Сложить – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.

  - Установить – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.

  - Получить – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.

  - Объединить – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.

  - Удалить – удалить запись из контекстной таблицы.

- Ключевые поля (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы. В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке **Селекторы**.

- Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.

- Сопоставление (требуется для всех операций, кроме **Удалить**) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.

- Левое поле используется для указания поля контекстной таблицы.

- Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

- Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

- Правое поле можно использовать для назначения константы полю контекстной таблицы, если была выбрана операция **Установить**. **Объединить** или **Сложить**. Максимальное количество символов – 1,024.

Вкладка **Корреляторы**

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Корреляторы**. После того как вы нажмете **OK**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок **Вверх** или **Вниз** установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Правила корреляции типа simple

Правила корреляции типа **simple** используются для определения простых последовательностей событий.

Окно правила корреляции содержит следующие вкладки параметров:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.

- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правила.

- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа правил.

- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Версия ресурса в репозитории "Лаборатории Касперского"** – номер версии ресурса. Это поле невозможно изменить. Поле доступно только для ресурсов, предоставляемых "Лабораторией Касперского", и используется для управления обновлениями ресурсов.

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.

- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **simple**, если хотите создать правило корреляции типа simple.

- **Наследуемые поля** (обязательно) – поля событий, по которым отбираются события. При срабатывания селектора (см. ниже) эти поля будут записаны в корреляционное событие.

- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Приоритет** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию – `Низкий`.

- **Описание** – описание ресурса. До 4000 символов Юникода.

Вкладка **Селекторы**

В правиле типа **simple** может быть только один селектор, для которого доступны вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр.

  Создание фильтра в ресурсах

Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

      Операторы фильтров

      - **=** – левый операнд равен правому операнду.
      - **<** – левый операнд меньше правого операнда.
      - **<=** – левый операнд меньше или равен правому операнду.
      - **>** – левый операнд больше правого операнда.
      - **>=** – левый операнд больше или равен правому операнду.
      - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
      - **contains** – левый операнд содержит значения правого операнда.
      - **startsWith** – левый операнд начинается с одного из значений правого операнда.
      - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
      - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
      - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

Последовательность условий, заданных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Рекомендуется на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.

Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.

Фильтр селектора 1:

Условие 1. DeviceProduct = Microsoft Windows

Условие 2. DeviceEventClassID = 4624

Фильтр селектора 2:

Условие 1. DeviceEventClassID = 4624

Условие 2. DeviceProduct = Microsoft Windows

Последовательность условий, заданная в Фильтре селектора 2, более предпочтительна, поскольку оказывает меньшую нагрузку на систему.

Выбрав вкладку **Локальные переменные**, с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Вкладка **Действия**

В правиле типа **simple** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- **В дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на постобработку: на обогащение, для реагирования и в точки назначения.

- **В коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться цепочкой правил текущего коррелятора. Это позволяет достичь иерархической корреляции.

  Если установлены флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции сначала отправляется на постобработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции. Если вы не хотите создавать алерт при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Не создавать алерт**. Если вы установите только флажок **Не создавать алерт**, событие корреляции не сохраняется в хранилище.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения. Эти правила обогащения хранятся в правиле корреляции, в котором они были созданы. Можно создать несколько правил обогащения. Вы можете добавлять или удалять правила обогащения с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - **константа**

      Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

      - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

      - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

    - **dictionary**

      Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.

  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.

- Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

  Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

  Доступные преобразования:

  - **lower** – используется для перевода всех символов значения в нижний регистр
  - **upper** – используется для перевода всех символов значения в верхний регистр
  - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
  - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
  - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
    - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
  - **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
  - **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
  - **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
  - **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
    - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

- **hexToDecimal** преобразует шестнадцатеричное числовое значение в его десятичное представление. Преобразование применяется к строковым или числовым полям, содержащим шестнадцатеричные значения (включая префикс 0x, если он есть), а результат сохраняется в поле целевого события KUMA в виде целого числа. Преобразование возвращает десятичное число. Например, значение 0x00FF преобразуется в 255.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразований.

- Для полей с типами `Число`, `Число с плавающей точкой` доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.

- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбран тип **Событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом `Массив строк`, а целевым полем является поле с типом `Строка`, значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем `Массив строк` и целевое поле полем `Массив строк`, значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

  - В поле **Шаблон** поместите шаблон Go.

    Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

    Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

  Если вы используете обогащения событий, у которого в качестве параметра **Тип источника** данных выбран тип **Шаблон**, в котором целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

  Пример:

  {{.SA.StringArrayOne}}

  Пример:

  {{- range $index, $element := . SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Отладка** – с помощью этого переключателя можно включить логирование операций сервиса.

- **Описание** – описание ресурса. До 4000 символов Юникода.

- Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько. Вы можете добавлять или удалять правила категоризации с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.

  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:

    - **Добавить** – присвоить категорию активу.

    - **Удалить** – отвязать актив от категории.

  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.

  - **Идентификатор категории** – в раскрывающемся списке отображается дерево категорий и вы можете выбрать категорию, над которой будет совершена операция. Список раскрывается, если нажать на строку.

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора активного листа.

  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:

    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.

    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.

    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

    - **Удалить** – удалить запись из активного листа.

  - **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

    > Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
  - Левое поле используется для указания поля активного листа.

    Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.
  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров Обновление контекстных таблиц – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок **Добавить действие с контекстной таблицей** и **Удалить действие с контекстной таблицей** можно добавлять и удалять операции с контекстными таблицами.
- Доступные параметры:
- Название (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.
- Операция (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.
- Сложить – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.
- Установить – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.
- Получить – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.
- Объединить – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.
- Удалить – удалить запись из контекстной таблицы.
- Ключевые поля (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы. В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке **Селекторы**.
- Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.
- Сопоставление (требуется для всех операций, кроме **Удалить**) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.
- Левое поле используется для указания поля контекстной таблицы.

- Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

- Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

- Правое поле можно использовать для назначения константы полю контекстной таблицы, если была выбрана операция **Установить**. **Объединить** или **Сложить**. Максимальное количество символов – 1,024.

Вкладка Корреляторы

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Корреляторы**. После того как вы нажмете **OK**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок Вверх или Вниз установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Правила корреляции типа operational

Правила корреляции типа **operational** используются для работы с активными листами.

Окно правила корреляции содержит следующие вкладки:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.

- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правил.

- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа правил.

- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Версия ресурса в репозитории "Лаборатории Касперского"** – номер версии ресурса. Это поле невозможно изменить. Поле доступно только для ресурсов, предоставляемых "Лабораторией Касперского", и используется для управления обновлениями ресурсов.

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **operational**, если хотите создать правило корреляции типа operational.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Описание** – описание ресурса. До 4000 символов Юникода.

Вкладка **Селекторы**

В правиле типа **operational** может быть только один селектор, для которого доступны вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр.

  Создание фильтра в ресурсах

  Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

  Чтобы создать фильтр:

  1. В раскрывающемся списке **Фильтр** выберите **Создать**.
  2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят.
  3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **Оператор** выберите оператор.

      Операторы фильтров

      - **=** – левый операнд равен правому операнду.
      - **<** – левый операнд меньше правого операнда.
      - **<=** – левый операнд меньше или равен правому операнду.
      - **>** – левый операнд больше правого операнда.
      - **>=** – левый операнд больше или равен правому операнду.
      - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
      - **contains** – левый операнд содержит значения правого операнда.
      - **startsWith** – левый операнд начинается с одного из значений правого операнда.
      - **endsWith** – левый операнд заканчивается одним из значений правого операнда.
      - **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
      - **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

        Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

        Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
      - **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

        Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
      - **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
      - **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

На вкладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Вкладка **Действия**

В правиле типа **operational** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
    - **Удалить** – удалить запись из активного листа.
  - **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

    Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для операции **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
  - Левое поле используется для указания поля активного листа.

    Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.
  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров **Обновление контекстных таблиц** – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок **Добавить действие с контекстной таблицей** и **Удалить действие с контекстной таблицей** можно добавлять и удалять операции с контекстными таблицами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.
    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.
    - **Установить** – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.
    - **Объединить** – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.
    - **Удалить** – удалить запись из контекстной таблицы.
  - **Ключевые поля** (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы. В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке Селекторы.

    Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.

  - **Сопоставление** (требуется для всех операций, кроме **Удалить**) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.
    - Левое поле используется для указания поля контекстной таблицы.

      Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

- Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

- Правое поле можно использовать для назначения константы полю контекстной таблицы. Максимальное количество символов – 1024.

Вкладка Корреляторы

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Корреляторы**. После того как вы нажмете **OK**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок Вверх или Вниз установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Переменные в корреляторах

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными *переменными*. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменные можно объявить в корреляторе (*глобальные переменные*) или в правиле корреляции (*локальные переменные*), присвоив им какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Область применения переменных:

- При поиске группирующих или уникальных значений полей в правилах корреляции.

- В селекторах правил корреляции в фильтрах условий, при которых должно срабатывать правило корреляции.

- При обогащении корреляционных событий. В качестве типа источника следует выбирать **Событие**.

- При наполнении активных листов значениями.

К переменным можно обращаться так же, как к полям события, предваряя их название символом $.

Локальные переменные в группирующих и уникальных полях

Вы можете использовать локальные переменных в разделах **Группирующие поля** и **Уникальные поля** правил корреляции типа standard. Для использования локальной переменной необходимо перед ее именем указывать символ "$".

Вы можете ознакомиться с примером использования локальных переменных в разделах **Группирующие поля** и **Уникальные поля** в правиле, поставляемом в KUMA: R403_Обращение на вредоносные ресурсы с устройства с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в селекторе

Чтобы использовать локальную переменную в селекторе:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Селекторы**, выберите существующий фильтр или создайте новый и нажмите на кнопку **Добавить условие.**
4. В качестве операнда выберите **поле события**.
5. В качестве значения поля события укажите локальную переменную и укажите символ "$" перед именем переменной.
6. Укажите остальные параметры фильтра.
7. Нажмите на кнопку **Сохранить**.

Вы можете ознакомиться с примером использования локальных переменных в правиле, поставляемом с KUMA: R403_Обращение на вредоносные ресурсы с устройства с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в обогащении событий

Вы можете использовать правила корреляции типа standard и simple для обогащения событий с помощью локальных переменных.

Обогащение текстом и числами

Обогащение событий можно выполнять с помощью текста (строк). Для этого могут быть использованы функции, позволяющие модифицировать строки: to_lower, to_upper, str_join, append, prepend, substring, tr, replace, str_join.

Обогащение событий можно выполнять с помощью чисел. Для этого могут быть использованы функции: сложение (оператор "+"), вычитание (оператор "-"), умножение (оператор "*"), деление (оператор "/"), round, ceil, floor, abs, pow.

Также для работы с данными в локальных переменных могут быть использованы регулярные выражения.

Применение регулярных выражений в правилах корреляции создает большую нагрузку в сравнении с другими операциями. Поэтому при разработке правил корреляции рекомендуется ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Обогащение временных отметок

Обогащение событий можно выполнять с помощью временных отметок (даты и времени). Для этого могут быть использованы функции, позволяющие получать или модифицировать временные метки: now, extract_from_timestamp, parse_timestamp, format_timestamp, truncate_timestamp, time_diff.

Операции с активными списками и таблицами

Вы можете выполнять обогащение событий с помощью локальных переменных и данных, находящихся в активных списках и таблицах.

Для обогащения событий данными из активного списка необходимо воспользоваться функциями active_list, active_list_dyn.

Для обогащения событий данными из таблицы необходимо воспользоваться функциями table_dict, dict.

Вы можете создавать условные операторы при помощи функции conditional в локальных переменных. Таким образом переменная может вернуть одно из значений в зависимости от того, какие данные поступили для обработки.

Использование локальной переменной для обогащения событий

Чтобы использовать локальную переменную для обогащения событий:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обогащение** в раскрывающемся списке **Тип источника данных** выберите **событие**.
4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое необходимо передать значение локальной переменной.
5. В раскрывающемся списке **Исходное поле** выберите локальную переменную. Перед именем локальной переменной укажите символ "$".
6. Укажите остальные параметры правила.
7. Нажмите на кнопку **Сохранить**.

Локальные переменные в обогащении активных листов

Вы можете использовать локальные переменные для обогащения активных листов.

Чтобы выполнить обогащение активного списка при помощи локальной переменной:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обновление активных листов** добавьте локальную переменную в поле **Ключевые поля**. Перед именем локальной переменной укажите символ "$".

4. В группе параметров **Сопоставление** укажите соответствие между полями события и полями активного списка.

5. Нажмите на кнопку **Сохранить**.

Свойства переменных

Локальные и глобальные переменные

Свойства глобальных и локальных переменных различаются.

Глобальные переменные:

- Глобальные переменные объявляются на уровне коррелятора и действуют только в пределах этого коррелятора.
- К глобальным переменным коррелятора можно обращаться из всех правил корреляции, которые в нем указаны.
- В правилах корреляции типа standard одна и та же глобальная переменная в каждом селекторе может принимать разные значения.
- Невозможно переносить глобальные переменные между разными корреляторами.

Локальные переменные:

- Локальные переменные объявляются на уровне правила корреляции и действуют только в пределах этого правила.
- В правилах корреляции типа standard областью действия локальной переменной является только тот селектор, в котором переменная была объявлена.
- Локальные переменные можно объявлять в любых типах правил корреляции.
- Невозможно переносить локальные переменные между правилами или селекторами.
- Локальная переменная не может быть использована в качестве глобальной переменной.

Переменные в разных типах правил корреляции

- В правилах корреляции типа **operational** на вкладке **Действия** можно указывать все доступные или объявленные в этом правиле переменные.
- В правилах корреляции типа **standard** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Группирующие поля**.
- В правилах корреляции типа **simple** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Наследуемые поля**.

Требования к переменным

Добавляя функцию переменной необходимо сначала указать название функции, а затем в круглых скобках перечислить ее параметры. Основные математические операции (сложение, вычитание, умножение, деление) являются исключением для этого требования. Когда используются эти операции, скобки используются для обозначения значимости операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Имя должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

Особенности указания функций переменных:

- Последовательность указания параметров имеет значение.
- Параметры передаются через запятую: `,`.
- Строковые параметры передаются в одинарных кавычках: `'`.
- Наименования полей событий и переменные указываются без кавычек.
- При обращении к переменной как параметру перед ее названием необходимо добавлять символ `$`.
- Ставить пробел между параметрами необязательно.
- Во всех функциях, где в качестве параметров допускается использование переменной, допускается создавать вложенные функции.

Функции переменных

Операции с активными листами и словарями

Функции active_list и active_list_dyn

Функции позволяют получать информацию из активного листа и динамически формировать имя поля активного листа и ключа.

Необходимо указать параметры в следующей последовательности:

1. Название активного листа.
2. Выражение, возвращающее название поля активного листа.
3. Одно или несколько выражений, из результатов которых будет составлен ключ.

Пример использования	Результат выполнения
`active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))`	Получение значения поля активного листа.

С помощью этих функций из переменной можно обратиться к активному листу общего тенанта. Для этого после названия активного листа необходимо добавить суффикс @Shared (регистр имеет значение). Например, active_list('exampleActiveList@Shared', 'score', SourceAddress, SourceUserName).

Функция table_dict

Получение информации о значении в указанном столбце словаря типа таблица.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.
2. Название столбца словаря.
3. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`table_dict('exampleTableDict', 'office', SourceUserName)`	Получение данных из словаря `exampleTableDict` из строки с ключом `SourceUserName` из столбца `office`.
`table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleTableDict` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре из столбца `office`.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `table_dict('exampleTableDict@Shared', 'office', SourceUserName)`.

Функция dict

Получение информации о значении в указанном столбце словаря типа словарь.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.
2. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`dict('exampleDictionary', SourceAddress)`	Получение данных из словаря `exampleDictionary` из строки с ключом `SourceAddress`.
`dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleDictionary` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `dict('exampleDictionary@Shared', SourceAddress)`.

Операции с контекстными таблицами

Функция context_table

Возвращает значение указанного поля в базовом типе (например, целое число,массив целых чисел).

Необходимо указать параметры в следующей последовательности:

1. Название контекстной таблицы. Название не должно быть пустым.
2. Выражение, возвращающее название поля контекстной таблицы.
3. Выражение, возвращающее название ключевого поля 1 контекстной таблицы.
4. Выражение, возвращающее значение ключевого поля 1 контекстной таблицы.

Функция должна содержать минимум 4 параметра.

Пример использования	Результат выполнения
`context_table('tbl1', 'list_field1', 'key1', 'key1_val')`	`Получение значения указанного поля. В случае отсутствия контекстной таблицы или поля контекстной таблицы будет получена пустая строка.`

Функция len

Возвращает длину строки и массива.

Функция возвращает длину массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает длину полученной строки.

Примеры использования
`len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`len(DeviceCustomString1)`

Функция distinct_items

Возвращает список уникальных элементов массива.

Функция возвращает список уникальных элементов массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;

- массив строк;
- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку, состоящую из уникальных символов исходной строки.

Примеры использования
`distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`distinct_items(DeviceCustomString1)`

Функция sort_items

Возвращает отсортированный список элементов массива.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект сортировки.
2. Сортировка возможных значений: `asc`, `desc`. Если параметр не указан, значение по умолчанию – `asc`.

Функция возвращает отсортированный список элементов массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк.

Функция возвращает список элементов массива в исходном порядке, если был передан массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку отсортированных символов.

Примеры использования
`sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')`
`sort_items(DeviceCustomString1)`

Функция item

Возвращает элемент массива с указанным индексом или символ строки с указанным индексом, если передан массив целых чисел, чисел с плавающей точкой, строк или булевых значений.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект индексирования.
2. Выражение, возвращающее индекс элемента или символа.

Функция должна содержать минимум 2 параметра.

Функция возвращает элемент массива с указанным индексом или символ строки с указанным индексом, если индекс находится в диапазоне массива и переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа и индекс находится в диапазоне массива, данные приводятся к строковому типу и функция возвращает символ строки по индексу. Если передан массив другого типа и индекс не находится в диапазоне массива, функция возвращает пустую строку.

Примеры использования
`item(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 1)`
`item(DeviceCustomString1, 0)`

Операции со строками

Функция to_lower

Перевод символов в строке в нижний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_lower(SourceUserName)`
`to_lower('SomeText')`
`to_lower($otherVariable)`

Функция to_upper

Перевод символов в строке в верхний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`. Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_upper(SourceUserName)`
`to_upper('SomeText')`
`to_upper($otherVariable)`

Функция append

Добавление символов в конец строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`append(Message, '123')`	Строка из поля `Message`, в конце которой добавлена строка `123`.
`append($otherVariable, 'text')`	Строка из переменной `otherVariable`, в конце которой добавлена строка `text`.
`append(Message, $otherVariable)`	Строка из поля `Message`, в конце которой добавлена строка из переменной `otherVariable`.

Функция prepend

Добавление символов в начало строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`prepend(Message, '123')`	Строка из поля `Message`, в начало которой добавлена строка `123`.
`prepend($otherVariable, 'text')`	Строка из переменной `otherVariable`, в начало которой добавлена строка `text`.
`prepend(Message, $otherVariable)`	Строка из поля `Message`, в начало которой добавлена строка из переменной `otherVariable`.

Функция substring

Возвращает подстроку из строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Позиция начала подстроки (натуральное число или 0).

3. Позиция конца подстроки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если номер позиции больше, чем длина строки исходных данных, возвращается пустая строка.

Примеры использования	Результат использования
`substring(Message, 2)`	Возвращает часть строки из поля `Message`: от 3 символа до конца.

`substring($otherVariable, 2, 5)`	Возвращает часть строки из переменной `otherVariable`: от 3 до 6 символа.
`substring(Message, 0, len(Message) - 1)`	Возвращает всю строку из поля `Message`, кроме последнего символа.

Функция index_of

Функция `index_of` возвращает байтовое смещение символа или подстроки в строке, расчет индекса начинается с 0. Если в результате работы функции подстрока не была найдена, функция вернет отрицательное значение.

Если в строке есть символы, не входящие в набор ASCII, то возвращаемое байтовое смещение не будет соответствовать количеству букв до искомой подстроки.

Доступны следующие параметры функции:

- В качестве исходных данных – поле события, другая переменная или константа.
- Любое выражение, которое доступно в локальных переменных.

Для использования функции необходимо указать параметры в следующей последовательности:

1. Символ или подстрока, позиция которой будет найдена.
2. Строка, по которой будет осуществлен поиск.

Примеры использования	Результат использования
`index_of('@', SourceUserName)`	Выполняется поиск символа `@` в поле `SourceUserName`. Поле `SourceUserName` содержит строку `user@example.com`. Результат = 4. Функция возвращает индекс первой позиции искомого символа в строке. Расчет индекса начинается с 0.
`index_of('m', SourceUserName)`	Выполняется поиск символа `m` в поле `SourceUserName`. Поле `SourceUserName` содержит строку `user@example.com`. Результат = 8. Функция возвращает индекс первой позиции искомого символа в строке. Расчет индекса начинается с 0.

Функция last_index_of

Функция `last_index_of` возвращает последнюю позицию символа или подстроки в строке, расчет индекса начинается с 0. Если в результате работы функции подстрока не была найдена, функция вернет значение -9223372036854775808.

Доступны следующие параметры функции:

- В качестве исходных данных – поле события, другая переменная или константа.
- Любое выражение, которое доступно в локальных переменных.

Для использования функции необходимо указать параметры в следующей последовательности:

1. Символ или подстрока, позиция которой будет найдена.
2. Строка, по которой будет осуществлен поиск.

Примеры использования	Результат использования
`last_index_of('m', SourceUserName)`	Выполняется поиск символа `m` в поле `SourceUserName`. Поле `SourceUserName` содержит строку `user@example.com`. Результат = 15. Функция возвращает индекс последней позиции искомого символа в строке. Расчет индекса начинается с 0.

Функция tr

Убирает из начала и конца строки указанные символы. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка, которую следует удалить из начала и конца исходной строки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если строку на удаление не указать, в начале и в конце исходной строки будут удалены пробелы.

Примеры использования	Результат использования
`tr(Message)`	В начале и в конце строки из поля `Message` удалены пробелы.
`tr($otherVariable, '_')`	Если переменной `otherVariable` соответствует значение `_test_`, будет возвращена строка `test`.
`tr(Message, '@example.com')`	Если в поле события `Message` находится строка `user@example.com`, будет возвращена строка `user`.

Функция replace

Заменяет все вхождения последовательности символов A в строке на последовательность символов B. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: последовательность символов, подлежащая замене.
3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска.

Строки можно передать выражением.

Примеры использования	Результат использования
`replace(Name, 'UserA', 'UserB')`	Возвращается строка из поля события `Name`, в которой все вхождения `UserA` заменены на `UserB`.
`replace($otherVariable, ' text ', '_text_')`	Возвращается строка из переменной `otherVariable`, в которой все вхождения `' text '` заменены на `'_text_'`.

Функция regexp_replace

Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Строка поиска: регулярное выражение.

3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска, и идентификаторы групп захвата регулярного выражения. Строку можно передать выражением.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования	Результат использования
`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	Возвращается строка из поля события `SourceAddress`, в которой перед IP-адресами вставлен текст `newIP`. Также последние цифры адреса заменены на `10`.

Функция regexp_capture

Получение из исходной строки результата, удовлетворяющего условию регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа `string`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Строка поиска: регулярное выражение.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования	Примеры значений	Результат использования
`regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')`	`Message = 'Access from 192.168.1.1 session 1'` `Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'`	`'192.168.1.1'` `'45.45.45.45'`

Функция template

Возвращает строку, указанную в функции, с заменой переменных на их значения. Переменные для подстановки можно передать следующими способами:

- Внутри строки.
- После строки. В этом случае необходимо в строке указать переменные типа `{{index.<n>}}`, где <n> – это индекс переменной после строки. Индекс начинается с 0.

Примеры использования
`template('текст со значениями полей события rule={{.DeviceCustomString1}} и {{.Name}}, а также значениями локальных переменных {{index.0}} и {{index.1}} и {{index.2}}', $var1, $var2, $var10)`

Операции с метками времени

Функция now

Получение временной метки в формате epoch. Запускается без аргументов.

Примеры использования
`now()`

Функция extract_from_timestamp

Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных с временем в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение атомарного представления времени. Параметр регистрозависимый.

   Возможные варианты обозначения атомарного времени:

   - y – год в виде числа.
   - M – месяц, числовое обозначение.
   - d – число месяца.
   - wd – день недели: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h – часы в 24-часовом формате.
   - m – минуты.
   - s – секунды.
3. Обозначение часового пояса (необязательно).

   Параметр может быть указан как строка (например, `Европа / Москва`) или как переменная (`$timezone`). Переменная должна быть объявлена в локальных переменных правила корреляции. Значение переменной должно содержать строковый идентификатор часового пояса. Также разрешено использовать переменные, производные от других переменных и значений словаря.

Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`extract_from_timestamp(Timestamp, 'wd')`
`extract_from_timestamp(Timestamp, 'h')`
`extract_from_timestamp($otherVariable, 'h')`
`extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`
`extract_from_timestamp(Timestamp, 'h', $timezone)`

Пример использования: использование переменной, полученной из словаря

`$key_timezone = 'timezone'`
 	
`$timezone = dict('UEBA.Timezone', $key_timezone)`
 	
`extract_from_timestamp(EndTime, 'h', $timezone)`

В этом примере переменная `$timezone` является производной от другой переменной и значения словаря и используется в качестве параметра `timezone`.

Функция parse_timestamp

Представление времени из формата RFC3339 (например, `2022-05-24 00:00:00`, `2022-05-24 00:00:00+0300`) в формат epoch.

Примеры использования
`parse_timestamp(Message)`
`parse_timestamp($otherVariable)`

Функция format_timestamp

Представление времени из формата epoch в формат RFC3339.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение формата времени: RFC3339.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`format_timestamp(Timestamp, 'RFC3339')`
`format_timestamp($otherVariable, 'RFC3339')`
`format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')`

Функция truncate_timestamp

Округление времени в формате epoch. После округления время возвращается в формате epoch. Время округляется в меньшую сторону.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Параметр округления:
   - 1s – округление до секунд;
   - 1m – округление до минут;
   - 1h – округление до часов;
   - 24h – округление до суток.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Примеры использования	Примеры округляемых значений	Результат использования
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654631760000 (7 June 2022 г., 19:56:00)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654628400000 (7 June 2022 г., 19:00:00)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654560000000 (7 June 2022 г., 0:00:00)

Функция time_diff

Получение интервала времени между двумя метками времени в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Время конца отрезка. Поле события, имеющего тип timestamp, или переменная.
2. Время начала отрезка. Поле события, имеющего тип timestamp, или переменная.
3. Представление временного интервала:
   - ms – в миллисекундах;
   - s – в секундах;
   - m – в минутах;
   - h – в часах;
   - d – в днях.

Примеры использования
`time_diff(EndTime, StartTime, 's')`
`time_diff($otherVariable, Timestamp, 'h')`
`time_diff(Timestamp, DeviceReceiptTime, 'd')`

Математические операции

Представлены как простейшими математическими операциями, так и функциями.

Простейшие математические операции

Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Операции:

- сложение;
- вычитание;
- умножение;
- деление;
- деление по модулю.

Использование круглых скобок определяет последовательность действий

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- вещественные числа.

  При делении по модулю в качестве аргументов можно использовать только натуральные числа.

Ограничения использования:

- Деление на ноль возвращает ноль.
- Математические операции между числами и строками возвращают число в неизменном виде. Например, "1 + abc" вернет 1.
- Целые числа, полученные в результате операций, возвращаются без точки.

Примеры использования (`Type=3; otherVariable=2; Message=text`)	Результат использования
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

Функция round

Округление чисел. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)	Результат использования
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

Функция ceil

Округление чисел в большую сторону. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
`ceil(DeviceCustomFloatingPoint1)`	8
`ceil($otherVariable)`	9

Функция floor

Округление чисел в меньшую сторону. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
`floor(DeviceCustomFloatingPoint1)`	7
`floor($otherVariable)`	8

Функция abs

Получение числа по модулю. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomNumber1=-7; otherVariable=-2)	Результат использования
abs(DeviceCustomFloatingPoint1)	7
abs($otherVariable)	2

Функция pow

Возведение числа в степень. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. База – вещественные числа.
2. Степень – натуральные числа.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования
pow(DeviceCustomNumber1, DeviceCustomNumber2)
pow($otherVariable, DeviceCustomNumber1)

Функция str_join

Позволяет объединить несколько строк в одну с использованием разделителя. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. Разделитель. Строка.
2. Строка1, строка2, строкаN. Минимум 2 выражения.

Примеры использования	Результат использования
str_join('|', to_lower(Name), to_upper(Name), Name)	Строка.

Функция conditional

Позволяет получить одно значения в случае выполнения условия и другое значение, если условие не выполнится. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. Условие. Строка. Синтаксис аналогичен условиям в SQL Where. В условии можно использовать функции переменных KUMA и ссылаться на другие переменные.

2. Значение при выполнении условия. Выражение.

3. Значение при невыполнении условия. Выражение.

Поддерживаемые операторы:

- `AND`
- `OR`
- `NOT`
- `=`
- `!=`
- `<`
- `<=`
- `>`
- `>=`
- `LIKE` (передается регулярное выражение RE2, а не SQL-выражение)
- `ILIKE` (передается регулярное выражение RE2, а не SQL-выражение)
- `BETWEEN`
- `IN`
- `IS NULL` (проверка на пустое значение, например 0 или пустую строку)

Примеры использования (значение зависит от аргументов 2 и 3)
`conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')`
`conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')`
`conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')`

Операции для полей расширенной схемы событий

Для полей расширенной схемы событий типа `строка` поддерживаются следующие виды операций:

- Функция `len`
- Функция `to_lower`
- Функция `to_upper`
- Функция `append`
- Функция `prepend`
- Функция `substring`
- Функция `tr`
- Функция `replace`
- Функция `regexp_replace`
- Функция `regexp_capture`

Для полей расширенной схемы событий с типом "целое число" или "число с плавающей точкой" поддерживаются следующие виды операций:

- Простые математические операции:
- Функция `round`
- Функция `ceil`
- Функция `floor`
- Функция `abs`
- Функция `pow`
- Функция `str_join`
- Функция `conditional`

KUMA поддерживает для полей расширенной схемы событий с типом `массив целых чисел`, `массив чисел с плавающей точкой` и `массив строк` следующие виды функций:

- Получение i-го элемента массива. Пример: `item(<type>.someStringArray)`.
- Получение массива значений. Пример: `<type>.someStringArray`. Вернет `["string1", "string2", "string3"]`.
- Получение количества элементов в массиве. Пример: `len(<type>.someStringArray)`. Вернет `["string1", "string2"]`.

- Получение уникальных записей из массива. Пример: `distinct_items(<type>.someStringArray)`.
- Формирование строки с элементами массива в формате TSV. Пример: `to_string(<type>.someStringArray)`.
- Сортировка элементов массива. Пример: `sort_items(<type>.someStringArray)`.

  В примерах вместо `<type>` необходимо указать тип массива: NA для массива целых чисел, FA для массива чисел с плавающей точкой, SA для массива строк.

Для полей с типом `массив целых чисел` и `массив чисел с плавающей точкой` поддерживаются следующие функции:

- `math_min` – возвращает минимальный элемент массива. Пример: `math_min(NA.NumberArray)`, `math_min(FA.FloatArray)`.
- `math_max` – возвращает максимальный элемент массива. Пример: `math_max(NA.NumberArray)`, `math_max(FA.FloatArray)`.
- `math_avg` – возвращает среднее значение массива. Пример: `math_avg(NA.NumberArray)`, `math_avg(FA.FloatArray)`.

Объявление переменных

Для объявления переменных их необходимо добавить в коррелятор или правило корреляции.

Чтобы добавить глобальную переменную в существующий коррелятор:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Корреляторы**.
2. Выберите набор ресурсов соответствующего коррелятора.

   Откроется мастер установки коррелятора.
3. Выберите шаг мастера установки **Глобальные переменные**.
4. Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:
5. В окне **Переменная** введите название переменной.

   Требования к наименованию переменных

   - Должно быть уникально в рамках коррелятора.
   - Имя должно содержать от 1 до 128 символов Юникода.
   - Не может начинаться с символа $.
   - Должно быть написано в camelCase или CamelCase.
   - В окне **Значение** введите функцию переменной.

     Описание функций переменных.

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

6. Выберите шаг мастера установки **Проверка параметров** и нажмите **Сохранить**.

Глобальная переменная добавлена в коррелятор. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Чтобы добавить локальную переменную в существующее правило корреляции:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Правила корреляции**.

2. Выберите соответствующее правило корреляции.

   Откроется окно параметров правила корреляции. Параметры правила корреляции можно также открыть из коррелятора, в которое оно было добавлено, перейдя на шаг мастера установки **Корреляция**.

3. Откройте вкладку **Селекторы**.

4. В селекторе откройте вкладку **Локальные переменные**, нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Имя должно содержать от 1 до 128 символов Юникода.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     Описание функций переменных.

   Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

   Для правил корреляции типа standard повторите этот шаг для каждого селектора, в которым вы хотите объявить переменные.

5. Нажмите на кнопку **Сохранить**.

Локальная переменная добавлена в правило корреляции. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Добавленные переменные можно изменить или удалить. Если правило корреляции обращается к необъявленной переменной (например, если ее название было изменено), в качестве результата возвращается пустая строка.

Если вы измените название переменной, вам потребуется вручную изменить название этой переменной во всех правилах корреляции, где вы ее использовали.

Предустановленные правила корреляции

В поставку OSMP включены перечисленные в таблице ниже правила корреляции.

Предустановленные правила корреляции

Название правила корреляции	Описание
[OOTB] KATA alert	Используется для обогащения событий KATA.
[OOTB] Successful Bruteforce	Срабатывает после выявления успешной попытки аутентификации после множества неуспешных попыток аутентификации. Правило работает на основе событий демона sshd.
[OOTB][AD] Account created and deleted within a short period	Выявляет факты создания и последующего удаления учетных записей на устройствах на базе ОС Microsoft Windows.
[OOTB][AD] An account failed to log on from different hosts	Выявляет множественные неуспешные попытки аутентификации на различных устройствах.
[OOTB][AD] Granted TGS without TGT (Golden Ticket)	Выявляет подозрения на атаку типа Golden Ticket. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD][Technical] 4768. TGT Requested	Техническое правило, используется для формирования активного списка – [OOTB][AD] List of requested TGT. EventID 4768. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] Membership of sensitive group was modified	Работает на базе событий ОС Microsoft Windows.
[OOTB][AD] Multiple accounts failed to log on from the same host	Срабатывает после выявления множественных неуспешных попыток аутентификации на одном устройстве от имени разных учетных записей.
[OOTB][AD] Possible Kerberoasting attack	Выявляет подозрения на атаки типа Kerberoasting. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] Successful authentication with the same account on multiple hosts	Выявляет подключения на разных устройствах под одной учетной записью. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] The account added and deleted from the group in a short period	Выявляет добавление и последующее удаление пользователя из группы. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][Net] Possible port scan	Выявляет подозрения на сканирование порта. Правило работает на основе событий Netflow, Ipfix.
[OOTB] EDR IOA alert	Осуществляет мониторинг событий EDR и создает алерт при обнаружении события EDR, которое имеет признак сработавшего IOA-правила и помечено как алерт.
[OOTB] EDR IOA SB alert	Отслеживает события EDR и создает предупреждение при обнаружении события EDR, полученного в результате автоматического сканирования Sandbox.
[OOTB] OSMP Scanner detects	Отслеживает события аудита безопасности, создаваемые компонентом IRP, и создает оповещение при получении события одного из следующих типов: "Проверка хостов YARA", "Обнаружение Sandbox", "Обнаружение вредоносных приложений", "Проверка хостов IOC", "Проверка сервера YARA".
[OOTB] KEDR event monitoring	Отслеживает события аудита и создает алерт при срабатывании политики мониторинга источника событий.
[OOTB] Multiple login attempts to OSMP console using the same account	Обнаруживает попытки входа в консоль OSMP с использованием одной учетной записи и генерирует алерт в случае трех неудачных попыток аутентификации.

Добавление временного списка исключений для корреляционного правила

Пользователи, не имеющие прав на изменение правил корреляции в Консоли OSMP, могут создать временный список исключений (например, создать исключения для ложных срабатываний при управлении алертами). Пользователь с правами редактирования корреляционных правил может затем по необходимости добавить исключения в правило и удалить их из временного списка.

Чтобы добавить исключения в корреляционное правило при работе с алертами:

1. Перейдите в раздел **Алерты** и выберите необходимый алерт.
2. Нажмите на кнопку **Найти в событиях**.

   Отображаются события алерта на странице событий.
3. Откройте корреляционное событие.

   Откроется карточка события, в которой напротив каждого поля отобразится кнопка (стрелка) для добавления исключения.
4. Нажмите на кнопку и выберите **Добавить в исключение**.

   Открывается боковая панель с полями: **Корреляционное правило**, **Исключение**, **Алерт**, **Комментарий**.
5. Нажмите на кнопку **Создать**.

Правило исключения добавлено.

Исключение добавится во временный список. Этот список будет доступен всем, у кого есть права на чтение корреляционных правил, в разделе **Ресурсы** → **Правила корреляции** в панели инструментов списка правил по кнопке **Список исключений**. Если вы хотите посмотреть исключения конкретного правила, откройте карточку правила и перейдите на вкладку **Исключения**.

Список исключений содержит записи со следующими параметрами:

- `Исключение`

  Условие исключения.
- `Правило корреляции`

  Наименование корреляционного правила.
- `Алерт`

  Наименование алерта, из которого было добавлено исключение.
- `Тенант`

  Тенант, в рамках которого действует правило и исключение соответственно.
- `Условие`

  Формируется автоматически на основании выбранного поля корреляционного события.
- `дата создания`

  Дата и время добавления исключения.
- `Срок действия`

Дата и время, когда исключение будет автоматически удалено из списка.

- `Создан`

  Имя пользователя, который добавил исключение.
- `Комментарий`

После добавления исключения, корреляционное правило будет работать с учетом исключения в течение 7 дней по умолчанию. В разделе **Параметры** → **Общие** вы можете настроить время действия исключений, изменив параметр `corr_rule_exclusion_ttl_hours` в разделе **Свойства ядра**. Вы можете настроить длительность хранения исключений в часах и днях. Минимальное значение – 1 час, максимальное – 365 дней. Этот параметр доступен только для пользователя с ролью Главный администратор.

Чтобы поля из базовых событий переходили в корреляционные события, эти поля необходимо указать в карточке корреляционного правила на вкладке **Общие** в поле **Наследуемые поля**. Если поля базовых событий не будут отображены в корреляционном событии, поля нельзя будет добавить в исключения.

Чтобы удалить исключения из корреляционного правила:

1. Перейдите в раздел **Ресурсы** → **Правила корреляции**.
2. В панели инструментов списка правил нажмите на кнопку **Список исключений**.

   Откроется окно со списком исключений.
3. Выбрать нужные исключения и нажать на кнопку **Удалить**.

Исключения будут удалены из корреляционного правила.

KUMA генерирует аудит события по факту создания или удаления исключений. Вы можете просмотреть изменения параметров события в окне **Информация о событии**.

Конвертер правил Sigma

Конвертер правил Sigma преобразует правила корреляции в формат, поддерживаемый OSMP, и упрощает импорт простых правил для последующей доработки аналитиком.

Список операционных систем, на которых поддерживается работа конвертера правил Sigma, приведен в разделе Программные требования.

Чтобы использовать конвертер правил Sigma для преобразования правил корреляции, выполните следующие шаги:

1. Установите конвертер правил Sigma. Доступны следующие варианты установки:

   - **Установка конвертера правил Sigma с использованием docker и bash**

     Этот метод установки подходит для локальной установки веб-интерфейса конвертера.

     Для установки требуются последние версии bash и docker. Для подробной информации по развертыванию bash и docker обратитесь к официальной документации.

     Astra Linux 1.7 не поддерживается.

Чтобы выполнить установку:

1. Войдите в директорию с распакованным архивом и выполните одну из команд:

   - Чтобы установить конвертер на хост с адресом

     `0.0.0.0:8000`
     , выполните следующую команду:

     ```
     ./run.sh
     ```

   - Чтобы установить конвертер на хост с адресом

     `0.0.0.0:8888`
     , выполните следующую команду:

     ```
     ./run.sh <port>
     ```

     где:

     <port> – порт (порт по умолчанию `8000`).

   - Чтобы установить конвертер на хост с адресом

     `127.0.0.1:9999`
     , выполните следующую команду:

     ```
     ./run.sh <IP address>:<port>
     ```

     где:

     - <IP address> — IP-адрес слушающего интерфейса, по умолчанию

       `0.0.0.0`
       . Указывайте

       `127.0.0.1`
       для запуска только на локальном интерфейсе.

     - <port> – порт.

   Конвертер установлен.

- **Установка конвертера правил Sigma в среде, допускающей запуск образов docker**

  Этот способ установки использует предоставленный контейнер, позволяет создать сервис systemd и развернуть веб-интерфейс с помощью Kubernetes.

  Подойдет любой инструмент запуска контейнеров: docker, podman, cri-o. Установка заключается в загрузке образа контейнера и последующего запуска образа с указанием нужного порта.

Чтобы установить конвертер с помощью podman:

1. Загрузите образ контейнера:

   ```
   podman load --input "kuma-sigma-converter-x.x.x.tar
   ```

2. Запустите образ одним из следующих способов:

   - Запуск до нажатия Ctrl+C:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
     ```

   - Запуск в фоновом режиме:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
     ```

   Конвертер установлен.

- **Установка конвертера правил Sigma с использованием Python версии 3.10 и выше**

  Этот метод установки отличается наибольшей гибкостью и подходит опытным пользователям, поскольку вы можете адаптировать конвертер под свои потребности. В отличие от других методов, этот метод требует подключения к интернету для скачивания пакетов Python.

  Чтобы выполнить установку конвертера:

  1. Убедитесь, что установлен Python версии 3.10 или выше.

  2. Установите poetry для управления зависимостями Python. Для Ubuntu или Debian можно воспользоваться менеджером пакетов:

     ```
     sudo apt-get update
     sudo apt install pipx
     pipx install poetry
     ```

  3. Используйте poetry для настройки и запуска веб-интерфейса конвертера правил Sigma:

     ```
     cd sigconverter.io
     poetry install
     poetry run ./run.py
     ```

  4. В браузере перейдите на устройство, где установлен веб-интерфейс конвертера правил Sigma. Для локальной установки адрес будет следующим: http://127.0.0.1:8000 или http://0.0.0.0:8000.

  5. При необходимости вы можете указать переменные окружения `HOST` и `PORT`
     , чтобы настроить слушающий интерфейс и задать номер порта.

  Конвертер установлен.

  Поскольку конвертер правил Sigma представляет собой плагин для инфраструктуры pySigma, допускается использование

  pySigma-backend-kuma

  с другими стандартными инструментами sigma, не только настраиваемой версией

sigconverter.io

. Например:
sigma-cli – конвертер с интерфейсом командной строки.

sigconverter.io – исходный универсальный веб-интерфейс.

Ниже указаны файлы README для библиотек, представленных в исходном коде:

src/pySigma/README.md – инфраструктура и библиотека промышленного стандарта преобразования sigma.

src/pySigma-backend-kuma/README.md – плагин для pySigma, который реализует преобразование фильтров и запросов OSMP.

src/sigconverter.io/README.md – пользовательский веб-интерфейс.

После установки войдите в веб-интерфейс конвертера.

2. Адаптируйте правило корреляции в конвертере правил Sigma и скопируйте или импортируйте адаптированное правило в OSMP.

3. Перезапустите коррелятор, чтобы применить изменения.

Адаптированное вами правило корреляции применяется в корреляторе.

Подготовка правил Sigma

Чтобы конвертировать правило Sigma в правило корреляции:

1. Перед доработкой правила убедитесь, что соблюдены следующие требования:

   - Поскольку в предустановленных нормализаторах используется обогащение событий `to lower case` для полей, содержащих имена пользователей, имена хостов, имена процессов, рекомендуется в исходном правиле Sigma приводить соответствующие поля к нижнему регистру.

   - Не рекомендуется в условиях `contains` и подобных условиях писать комментарии или дополнительную информацию. В случае необходимости оставить комментарий рекомендуется использовать символ `#`, тогда комментарий не окажет влияния на условие.

   - Правило должно начинаться со слова `title`, дефисов перед ним не должно быть.

2. Скопируйте из веб-интерфейса OSMP правило корреляции, которое вы хотите доработать, конвертируйте его в формат YML и вставьте на вкладку конвертера **rule.yml**. Выберите в раскрывающихся списках нужные параметры. При необходимости исправьте ошибки.

3. В конвертере правил Sigma в поле **Backend** выберите **kuma**, в поле **Format** выберите **default**, поле **Pipeline** оставьте пустым.

   Доступны следующие значения:

   - Backend: kuma, Format: default – готовый для запуска SQL-запрос без форматирования.

   - Backend: kuma, format: SQL_formatted – готовый для запуска SQL запрос с форматированием.

- Backend: kuma_filter, Format: default – готовый селектор для правила корреляции.
- Backend: kuma_filter, Format: correlation – готовое для импорта правило корреляции в формате JSON. Для импорта вы можете использовать метод REST API /xdr/api/v3/kuma/resources/{kind}/create с указанием tenantID и названия тенанта для импорта.

4. Перейдите на вкладку конвертера **custom_pipeline.yml** и скопируйте на эту вкладку пример словаря, адаптированный под pySigma.

   Пример словаря, адаптированный под pySigma

   Windows process_creation mapping

   product: windows

   category: process_creation

   DeviceEventClassID = 4688

   Windows sysmon EVENT=11 mapping

   product: windows

   service: Sysmon

   EventID = 11

   Windows security

   product: windows

   service: security

   EventID = 4624|4662|4104|4698

```
name: KUMA windows
priority: 30
transformations:
### Windows process_creation mapping

  - id: MAPPING_logsource_windows_process_creation
    type: field_name_mapping
    mapping:
      ParentImage: SourceProcessName
      Image: DestinationProcessName
      CommandLine: DeviceCustomString4
    rule_conditions:
      - type: logsource
        product: windows
        category: process_creation

  - id: DEFAULT_FOR_logsource_windows_process_creation
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
      DeviceEventClassID: '4688'
    rule_conditions:
       - type: logsource
         product: windows
```

```
        category: process_creation

### Windows sysmon EventID=11 mapping
  - id: DEFAULT_FOR_logsource_windows_sysmon
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Sysmon
    rule_conditions:
       - type: logsource
         product: windows
         service: Sysmon

  - id: MAPPING_logsource_windows_sysmon
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Image: OldFilePath
      CommandLine: DeviceCustomString4
      TargetFilename: FilePath
    rule_conditions:
      - type: logsource
        product: windows
        service: Sysmon

### Windows security mapping
  - id: DEFAULT_FOR_logsource_windows_security
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: DEFAULT_MAPPING_FOR_logsource_windows_security
    type: field_name_mapping
    mapping:
      Computer: DestinationHostName
      LogonID: FlexString1
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: 4624_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      LogonType: DeviceCustomNumber1
      SourceIP: SourceAddress
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4624

  - id: 4662_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Properties: FilePermission
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4662

  - id: 4104_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      ScriptBlockText: Message
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4104

  - id: 4698_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      TaskName: SourceProcessName
```

```
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: '4698'
```

На вкладке **query** отобразится конвертированное правило. В результате конвертации вы получите условие `WHERE` для SQL-запроса.

Вы можете скопировать готовый результат в OSMP, если это запрос или фильтр. Если вы хотите использовать в OSMP правило, можно импортировать в OSMP по одному правилу.

Примеры поддерживаемых конвертаций правил Sigma

Поддерживаемые примеры конвертации правил Sigma

Правило Sigma	Сопоставление с объектами OSMP	

`title: Generic-DCSync Execution`
`id: 9107f781-c984-436a-8093-1aaa64c70c49`
`description: Detects access to DC with "DS-Replication-Get-Changes" or "DS-Replication-Get-Changes-All" rights`
`author: Kaspersky`
`status: stable`
`modified: 2023-08-02`
`tags:`
`  - attack.credential_access`
`  - attack.t1003.006`
`logsource:`
`  product: windows`
`  service: security`
`detection:`
`  selection1:`
`  EventID: 4662`
`  Properties|contains:`
`  - 'DS-Replication-Get-Changes'`
`  - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2'`
`  - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2'`
`  selection2:`
`  EventID: 4624`
`  LogonType: 3`
`  filter:`
`  EventID: 4624`
`  LogonType: 3`
`  SourceIP:`
`  - '<ip address of DC servers>'`
`  timeframe: 1m`
`  condition: selection1 or (selection2 and not filter) | count(EventID) by Computer,LogonID = 2`
`fields:`
`  - SourceIP`
`  - Computer`
`  - LogonID`
`  - Username`
`  - Properties`
`falsepositives:`
`- Unknown`
`level: high`
	Нормализатор "Microsoft products"
	`tags → description`
	`logsource`
	`DeviceVendor = Microsoft`
	
	`DeviceProduct = Windows`
	
	`selection1:`
	
	`DeviceEventClassID=4662`
	`FilePermission contains '' OR FilePermission contains '' OR FilePermission contains ''`
	`selection2`
	`DeviceEventClassID=4624`
	`DeviceCustomNumber1 = 3`
	`filter`
	`DeviceEventClassID=4624`
	`DeviceCustomNumber1 = 3`
	`SourceAddress = <IP>`
	`condition:`
	`DeviceVendor = Microsoft AND`
	
	`DeviceProduct = Windows AND`
	
	`((`
	`DeviceEventClassID=4662`
	`FilePermission contains '' OR FilePermission contains '' OR FilePermission contains ''`
	`) OR`
	`(`
	`(`
	`DeviceEventClassID=4624 AND`
	`DeviceCustomNumber1 = 3`
	`) NOT`
	`(`
	`DeviceEventClassID=4624 AND`
	`DeviceCustomNumber1 = 3 AND`
	`SourceAddress = <IP>`
	`)`
	`)`
	`)`
	
	`все, что внутри Count()`
	`EventID положить в Unique fields,`
	`все, что после 'by'`
	`Computer → DestinationHostName`
	`LogonID → FlexString1`
	`положить в Aggregation fields,`
	`все, что после '=' или '>'`
	`2 положить в threshold.`
	`timeframe`
	`положить в time window`
		Это корреляцион
		simple правило O
		частично: если уб
		можно получить у
		правила или SQL-

Правило Sigma	Сопоставление с объектами OSMP	
title: Lsass Dump via LOLBin id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02 description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe references: - https://twitter.com/bohops/status/1635288066909966338 - https://twitter.com/mrd0x/status/1511415432888131586 modified: 2023-07-18 author: Kaspersky status: stable tags: - attack.credential_access - attack.t1003.001 logsource: product: windows category: process_creation detection: selection_procdump: Image|endswith: - '\procdump.exe' - '\procdump64.exe' CommandLine|contains: 'lsass' selection_dotnet: Image|endswith: '\dotnet-dump.exe' CommandLine: ' collect ' selection_dumpminitool: Image|endswith: '\dumpminitool.exe' condition: 1 of selection* falsepositives: - Unknown level: high	Конвертируется так же, как и правило в строке 3 таблицы. Отличие: условие в condition 1 of selection* – одна из именованных коллекций.	DeviceVendor=' DeviceProduct= DeviceEventCla (((Desti '\\procdump.ex '\\procdump64. 'lsass') OR (Destinati dump.exe' AND De) OR Destinati '\\dumpminitoo)
title: Generic-Clearing Windows Event Logs via Command Line id: a903492e-da40-4ab4-a92d-306a4799d973 description: Detects Clear Windows Event Logs via Command Line author: Kaspersky status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1070.001 logsource: product: windows category: process_creation detection: selection1: Image|endswith: '\wevtutil.exe' CommandLine|contains: - ' cl ' - 'clear' selection2: Image|endswith: - '\powershell.exe' - '\powershell_ise.exe' - '\pwsh.exe' CommandLine|contains: - 'Clear-EventLog' - 'Remove-EventLog' selection3: Image|endswith: '\wmic.exe' CommandLine|contains: - 'ClearEventLog' condition: 1 of them falsepositives: - Legitimate System Administrator actions level: high	Нормализатор "Microsoft products" tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows DeviceEventClassID=4688 selection1: DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" Selection2 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" selection3 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" condition DeviceVendor = Microsoft AND DeviceProduct = Windows AND DeviceEventClassID=4688 AND ((DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains ""))) identical fields - указывать поля из условия за исключением полей Name, deviceProduct, deviceVendor	DeviceVendor=' DeviceProduct= DeviceEventCla ((Destinati '\\wevtutil.ex (Devic DeviceCustomSt) OR ((Destin '\\powershell. Des '\\powershell\ '\\pwsh.exe') (Device EventLog' OR D 'Remove-EventL) OR (Destinatio AND DeviceC 'ClearEventLog)

Правило Sigma	Сопоставление с объектами OSMP	
title: 0021-0002.1204.003 Execution - PowerExchangeDropper description: Detect the dropping of PowerExchange components. status: experimental logsource: product: windows service: Sysmon detection: selection1: EventID: 11 selection2: TargetFilename|contains: - 'c:\users\public\microsoftedge\autosave.exe' - 'c:\users\public\microsoftedge\wsdl.ps1' selection3: Image|endswith: "brochure.exe" condition: selection1 and selection2 and selection3 falsepositives: - Unknown level: high	Основание: Нормализатор 11 события Sysmon. title → name author → description description→ description status → description logsource DeviceVendor = Microsoft DeviceProduct = Sysmon selection1 DeviceEventClassID=11 selection2 FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '' если есть * пути к файлу форматировать в regexp selection3 OldFilePath endswith "" condition: DeviceVendor = Microsoft AND DeviceProduct = Sysmon AND (DeviceEventClassID=11) AND (FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '') AND (OldFilePath endswith "") identical fields – указывать поля из условия за исключением полей Name, deviceProduct, deviceVendor level →severity falsepositive → Description	DeviceVendor=' DeviceProduct= DeviceEventCla (FilePath con 'c:\\users\\pu OR FilePath c 'c:\\users\\pu) AND OldFilePath en
title: Domain joined host discovery description: Detect an attacker enumerating domain-joined machines using PowerShell. status: stable logsource: product: windows service: security detection: selection: EventID: 4104 ScriptBlockText|contains|all: - 'System.DirectoryServices.DirectorySearcher' - 'Properties.operatingsystem' condition: selection falsepositives: - "Administrative scripts or tools like Vulnerability Scanners" level: medium	ScriptBlockText → Message	

Правило Sigma	Сопоставление с объектами OSMP	
title: 0022-0002.1053.005 Execution - PowerExchange Task description: Detect the creation of a scheduled task by PowerExchange. status: experimental logsource: product: windows service: security detection: selection: EventID: - '4698' TaskName|contains: - 'MicrosoftEdgeUpdateService' condition: selection falsepositives: - Unknown level: medium	TaskName → SourceProcessName	

Правило Sigma	Сопоставление с объектами OSMP	
title: Created Windows Shell from Critical Windows Process description: Anomaly behavior critical windows process status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1036 logsource: product: windows category: process_creation detection: selection: ParentImage|endswith: - '\searchindexer.exe' - '\lsaiso.exe' - '\lsm.exe' - '\spoolsv.exe' - '\wininit.exe' - '\smss.exe' - '\csrss.exe' - '\lsass.exe' - '\services.exe' - '\winlogon.exe' Image|endswith: - '\powershell_ise.exe' - '\cmstp.exe' - '\appvlp.exe' - '\mftrace.exe' - '\scriptrunner.exe' - '\forfiles.exe' - '\msiexec.exe' - '\rundll32.exe' - '\mshta.exe' - '\hh.exe' - '\wmic.exe' - '\regsvr32.exe' - '\scrcons.exe' - '\bash.exe' - '\sh.exe' - '\cscript.exe' - '\wscript.exe' - '\powershell.exe' - '\cmd.exe' condition: selection falsepositives: - Unknown level: high	ParentImage → SourceProcessName	

Покрытие матрицы MITRE ATT&CK

Если вы хотите оценить покрытие матрицы MITRE ATT&CK вашими корреляционными правилами, вам нужно выполнить следующее:

1. Скачать список техник MITRE из официального хранилища MITRE ATT&CK и импортируйте справочник техник MITRE в KUMA.
2. Сопоставить техники MITRE с правилами корреляции.
3. Экспортировать правила корреляции в MITRE ATT&CK Navigator.

В результате вы сможете визуально оценить покрытие матрицы MITRE ATT&CK.

Импорт списка техник MITRE

Импортировать список техник MITRE может только пользователь с ролью Главный администратор.

Чтобы импортировать список техник MITRE ATT&CK:

1. Скачайте справочник техник MITRE ATT&CK на портале GitHub.

   KUMA поддерживает только список техник MITRE ATT&CK версии 14.1.

2. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

3. В блоке **Другое** нажмите **Общие**.
4. В разделе **Параметры списка техник MITRE** нажмите на кнопку **Импортировать из файла**.

   Откроется окно выбора файлов.

5. Выберите скачанный список техник MITRE ATT&CK и нажмите на кнопку **Открыть**.

Список техник MITRE ATT&CK импортирован в KUMA. Вы можете увидеть список импортированных техник и версию списка техник MITRE ATT&CK, нажав на **Просмотреть список**.

Сопоставление техник MITRE с правилами корреляции

Чтобы сопоставить техники MITRE ATT&CK правилам корреляции:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Правила корреляции**.
2. Нажмите на имя правила корреляции, чтобы открыть окно свойств правила корреляции.

   Откроется окно свойств правила корреляции.

3. На вкладке **Общие** нажмите на поле **MITRE техника**, чтобы открыть список доступных техник. Для удобства поиска предусмотрен фильтр, в который можно ввести название техники или идентификатор техники или тактики. Одна или несколько техник MITRE ATT&CK доступны для сопоставления с правилом корреляции.

4. Нажмите на кнопку **Сохранить**.

Техники MITRE ATT&CK сопоставлены с правило корреляции. В Консоли KUMA в разделе **Мониторинг** → **Ресурсы** → **Правила корреляции** в столбце **Техники MITRE** у измененного правила отобразится идентификатор выбранной техники, а при наведении курсора на идентификатор отобразится полное название техники с указанием идентификатора техники и тактики.

Экспорт правила корреляции в MITRE ATT&CK Navigator

Чтобы экспортировать правила корреляции с сопоставленными техниками MITRE в MITRE ATT&CK Navigator:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Правила корреляции**.

2. В правом верхнем углу нажмите на кнопку с многоточием (...).

3. В раскрывающемся списке нажмите на кнопку **Экспортировать в MITRE ATT&CK Navigator**.

4. В открывшемся окне выберите нужное правило корреляции, которое вы хотите экспортировать.

5. Нажмите на кнопку **OK**.

   На ваше устройство будет загружен файл с экспортированными правилами.

6. Загрузите файл с вашего компьютера в MITRE ATT&CK Navigator для оценки покрытия матрицы MITRE ATT&CK.

Вы можете произвести проверку покрытия матрицы MITRE ATT&CK.

Фильтры

Фильтры позволяют выбрать события на основе заданных вами условий.

В сервисе коллектора фильтры используются для того, чтобы выбрать события, которые вы хотите передавать в KUMA. То есть если событие удовлетворяет условию фильтра, событие будет передано в KUMA для дальнейшей обработки.

Фильтры можно использовать в следующих сервисах и функциях KUMA:

- Коллектор.
- Коррелятор.
- Хранилище.
- Правила корреляции.
- Правила обогащения.

- Правила агрегации.
- Точки назначения.
- Правила реагирования.
- Правила сегментации.

Можно использовать отдельные фильтры или встроенные фильтры, которые хранятся в сервисе или ресурсе, где они были созданы.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Доступные параметры фильтра:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода. Встроенные фильтры создаются в других ресурсах или сервисах и не имеют имен.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Описание – вы можете добавить до 4000 символов Юникода, описывающих фильтр.
- Блок параметров **Условия** – здесь вы можете сформулировать критерии фильтрации, создав условия фильтрации и группы фильтров, а также добавив существующие фильтры.

  Для формирования критериев фильтрации вы можете использовать *режим конструктора* или *режим исходного кода*. По умолчанию используется режим конструктора.

  В режиме конструктора вы можете создавать или изменять критерии фильтрации с помощью раскрывающихся списков с вариантами условий фильтра и операторов.

  В режиме исходного кода вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

  Вы можете переключаться между режимами при формировании критериев фильтрации. Чтобы переключиться в режим исходного кода, нажмите на кнопку **Код**. При переключении между режимами созданные фильтры условий сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, перейдите на вкладку **Конструктор** и вернитесь снова на вкладку **Код**. Отобразится код фильтра.

Формирование условий в режиме конструктора

Вы можете формировать критерии фильтрации в режиме конструктора с помощью следующих кнопки:

- **Добавить условие** – добавление строки с полями для определения условия.
- **Добавить группу –** добавление группы фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить группы, условия и существующие фильтры. Условия, помещенные в подгруппу **НЕ**, объединяются оператором **И**.

Для замены в сформированном условии оператора вам необходимо нажать на оператор, который вы хотите заменить, и в раскрывающемся списке выбрать новый оператор.

Для удаления в сформированном условии оператора необходимо нажать на оператор, который вы хотите удалить, и нажать на клавишу **Backspace**.

Для изменения последовательности условий фильтра вам необходимо нажать на кнопку ⠿ и перетащить условие на новое место.

Условия, группы и фильтры можно удалить, нажав на кнопку ✕.

Параметры условий:

- **Если** (обязательно) – в этом раскрывающемся списке можно указать, требуется ли использовать инвертированную функцию оператора.

- **Левый операнд** и **Правый операнд** (обязательно) – используются для указания значений, которые будет обрабатывать оператор. Доступные типы зависят от выбранного оператора.

  Операнды фильтров

  - **Поле события** – используется для присвоения операнду значения поля события. Дополнительные параметры:

    - **поле события** (обязательно) – этот раскрывающийся список используется для выбора поля, из которого следует извлечь значение операнда.

  - **Активный лист** – используется для присвоения операнду значения записи активного листа. Дополнительные параметры:

    - **название активного листа** (обязательно) – этот раскрывающийся список используется для выбора активного листа.

    - **ключевые поля** (обязательно) – это список полей событий, используемых для создания записи активного листа и служащих ключом записи активного листа.

    - **поле** (требуется, если не выбран оператор **inActiveList**) – используется для ввода имени поля активного листа, из которого следует извлечь значение операнда.

  - **Контекстная таблица** – используется для присвоения операнду значения контекстной таблицы. Дополнительные параметры:

    - **название контекстной таблицы** (обязательно) – этот раскрывающийся список используется для выбора контекстной таблицы.

    - **ключевые поля** (обязательно) – это список полей событий или локальных переменных, используемых для создания записи контекстной таблицы и служащих ключом записи контекстной таблицы.

    - **поле** – используется для ввода имени поля контекстной таблицы, из которого следует извлечь значение операнда.

    - **индекс** – используется для ввода индекса списочного поля таблицы, из которого следует извлечь значение операнда.

  - **Словарь** – используется для присвоения значения операнду значения из ресурса словарь. Дополнительные параметры:

    - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря.

    - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.

- **Константа** – используется для присвоения операнду пользовательского значения. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите константу, которую хотите присвоить операнду.
- **Таблица** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря типа **Таблица**.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.
- **Список** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите список констант, которые хотите назначить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
- **TI** – используется для чтения данных CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – в этом поле указывается категория угрозы CyberTrace.
  - **ключевые поля** (обязательно) – этот раскрывающийся список используется для выбора поля события с индикаторами угроз CyberTrace.
  - **поле** (обязательно) – в этом поле указывается поле фида CyberTrace с индикаторами угроз.

- **Оператор** (обязательно) – используется для выбора оператора условия.

  В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **inSubnet**, **inActiveList**, **inCategory**, **InActiveDirectoryGroup, hasBit**, **inDictionary**. По умолчанию флажок снят.

  Операторы фильтров

  - **=** – левый операнд равен правому операнду.
  - **<** – левый операнд меньше правого операнда.
  - **<=** – левый операнд меньше или равен правому операнду.
  - **>** – левый операнд больше правого операнда.
  - **>=** – левый операнд больше или равен правому операнду.
  - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
  - **contains** – левый операнд содержит значения правого операнда.
  - **startsWith** – левый операнд начинается с одного из значений правого операнда.
  - **endsWith** – левый операнд заканчивается одним из значений правого операнда.

- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.

- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Доступные типы операндов зависят от того, является ли операнд левым (L) или правым (R).

Доступные типы операндов для левого (L) и правого (R) операндов

Оператор	Тип "поле события"	Тип "активный лист"	Тип "словарь"	Тип "контекстная таблица"	Тип "таблица"	Тип "TI"	Тип "константа"	Тип "список"
=	L,R	L,R	L,R	L,R	L,R	L,R	R	R
>	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
>=	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
<	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
<=	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—

inSubnet	L,R	L,R	L,R	L,R	L,R	L,R	R	R
contains	L,R	L,R	L,R	L,R	L,R	L,R	R	R
startsWith	L,R	L,R	L,R	L,R	L,R	L,R	R	R
endsWith	L,R	L,R	L,R	L,R	L,R	L,R	R	R
match	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

Вы можете использовать при работе с фильтрами горячие клавиши. Описание горячих клавиш приведено в таблице ниже.

Горячие клавиши и их функциональность

Клавиша	Функциональность
e	Вызывает фильтр по полю события
d	Вызывает фильтр по полю словаря
a	Вызывает фильтр по полю активного листа
c	Вызывает фильтр по полю контекстной таблицы
t	Вызывает фильтр по полю таблицы
f	Вызывает фильтр
t+i	Вызывает фильтр с использованием TI
Ctrl+Enter	Завершение редактирования условия

Работа с полями типа `строка`, `число` и `число с плавающей точкой` расширенной схемы событий в фильтрах не отличается от работы с полями схемы событий KUMA.

При использовании фильтров с полями расширенной схемы событий с типами полей `Массив строк`, `Массив целых чисел` и `Массив чисел с плавающей точкой` возможно использование следующих операций:

- Операция `contains` вернет значение `True`, если указанная подстрока присутствует в массиве, иначе вернет `False`.
- Операция `match` – поиск в строке по регулярному выражению.
- Операция `intersec`.

При использовании фильтров с полями расширенной схемы событий с типами полей `Массив целых чисел` и `Массив чисел с плавающей точкой` возможно использование следующих операций сравнения чисел: `<`, `>`, `=`, `>=`, `<=`.

Для обращения к конкретному элементу массива в фильтре необходимо использовать следующий синтаксис: `NA.<имя массива>.<номер элемента>`

Нумерация элементов массива начинается с 0.

Пример:

`NA.ArrayOne.0` – обращение к первому элементу массива чисел ArrayOne.

`FA.ArrayTwo.2` – обращение к третьему элементу массива чисел с плавающей точкой ArrayTwo.

Формирование условий в режиме исходного кода

Режим редактора кода позволяет быстро редактировать условия, выделять и копировать блоки кода.

В правой части конструктора отображается навигатор, позволяющий переместиться ко коду фильтра.

Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Для ресурсов, использованных в фильтре, автоматически указывается их наименование. Поля, содержащие наименования связанных ресурсов, нельзя отредактировать. Имена категорий общих ресурсов не отображаются в фильтре, если у вас нет роли **Чтение общих ресурсов**.

В поставку OSMP включены перечисленные в таблице ниже фильтры.

Предустановленные фильтры

Название фильтра	Описание
[OOTB][AD] A member was added to a security-enabled global group (4728)	Выбирает события добавления пользователя в группу безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was added to a security-enabled universal group (4756)	Выбирает события добавления пользователя в группу безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled global group (4729)	Выбирает события удаления пользователя из группы безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled universal group (4757)	Выбирает события удаления пользователя из группы безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] Account Created	Выбирает события создания учетной записи в ОС Windows.
[OOTB][AD] Account Deleted	Выбирает события удаления учетной записи в ОС Windows.
[OOTB][AD] An account failed to log on (4625)	Выбирает события неуспешной попытки входа в ОС Windows.
[OOTB][AD] Successful Kerberos authentication (4624, 4768, 4769, 4770)	Выбирает события успешной попытки входа в ОС Windows и события с идентификаторами 4769, 4770, регистрирующиеся на контроллерах домена.
[OOTB][AD][Technical] 4768. TGT Requested	Выбирает события Microsoft Windows с идентификатором 4768.
[OOTB][Net] Possible port scan	Выбирает события, которые могут говорить о проведении сканирования портов.
[OOTB][SSH] Accepted Password	Выбирает события успешного подключения с использование пароля по протоколу SSH.
[OOTB][SSH] Failed Password	Выбирает события попыток подключения с использование пароля по протоколу SSH.

Активные листы

Активный лист – это контейнер для данных, которые используются корреляторами KUMA при анализе событий по правилам корреляции.

Например, если у вас есть список IP-адресов с плохой репутацией, вы можете:

1. Создать корреляционное правило типа operational и добавить в активный лист эти IP-адреса.
2. Создать корреляционное правило типа standard и указать активный лист в качестве условия фильтрации.
3. Создать коррелятор с этим правилом.

   В этом случае KUMA выберет все события, которые содержат IP-адреса, внесенные в активный лист, и создаст корреляционное событие.

Вы можете наполнять активные листы автоматически с помощью корреляционных правил типа simple или импортировать файл с данными для активного листа.

Вы можете добавлять, копировать и удалять активные листы.

Активные листы можно использовать в следующих сервисах и функциях KUMA:

- Правила корреляции.
- Панель мониторинга.

Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

В активный лист добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, дублировать, удалять и экспортировать записи в активном листе коррелятора.

В процессе корреляции при удалении записей из активных листов в корреляторах создаются служебные события. Эти события существуют только в корреляторах, они не перенаправляются в другие точки назначения. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы. Поля служебных событий удаления записи из активного листа описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события
`Timestamp`	Время удаления записи, срок жизни которой истек.
`Имя`	`"active list record expired"`
`DeviceVendor`	`"Лаборатория Касперского".`
`DeviceProduct`	`"KUMA"`
`ServiceID`	Идентификатор коррелятора.
`ServiceName`	Название коррелятора.
`DeviceExternalID`	Идентификатор активного листа
`DevicePayloadID`	Ключ записи, чей срок жизни истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи
`S.<active list field>`	Запись активного листа в следующем формате: S.<поле активного листа> = <значение активного листа>

Просмотр таблицы активных листов

Чтобы просмотреть таблицу активных листов коррелятора:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя активного листа.
- **Записи** – количество записей в активном листе.
- **Размер на диске** – размер активного листа.
- **Директория** – путь к активному листу на сервере коррелятора KUMA.

Добавление активного листа

Чтобы добавить активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Активные листы**.
2. Нажмите на кнопку **Добавить активный лист**.
3. Выполните следующие действия:

   a. В поле **Название** введите имя активного листа.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   c. В поле **Срок жизни** укажите время, в течение которого в активном листе будет храниться добавленная в него запись.

   По истечении указанного времени запись удаляется. Время указывается в секундах.

   Значение по умолчанию – 0. Если в поле указано значение 0, запись хранится 36000 дней (около 100 лет).

   d. В поле **Описание** укажите любую дополнительную информацию.

   Вы можете использовать до 4000 символов Юникода.

Поле не является обязательным.

4. Нажмите на кнопку **Сохранить**.

Активный лист будет добавлен.

Просмотр параметров активного листа

Чтобы просмотреть параметры активного листа:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Активные листы**.
2. В столбце **Название** выберите активный лист, параметры которого вы хотите просмотреть.

Откроется окно с параметрами активного листа. В нем отображается следующая информация:

- **Идентификатор** – идентификатор активного листа.
- **Название** – уникальное имя ресурса.
- **Тенант** – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Значение указывается в секундах.
- **Описание** – любая дополнительная информация о ресурсе.

Изменение параметров активного листа

Чтобы изменить параметры активного листа:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Активные листы**.
2. В столбце **Название** выберите активный лист, параметры которого вы хотите изменить.
3. Укажите значения для следующих параметров:
   - **Название** – уникальное имя ресурса.
   - **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Значение указывается в секундах.

     Если в поле указано значение 0, запись хранится бессрочно.
   - **Описание** – любая дополнительная информация о ресурсе.

Поля **Идентификатор** и **Тенант** недоступны для редактирования.

Дублирование параметров активного листа

Чтобы скопировать активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Активные листы**.
2. Установите флажок рядом с активным листом, который вы хотите скопировать.
3. Нажмите на кнопку **Дублировать**.
4. Укажите нужные вам параметры.
5. Нажмите на кнопку **Сохранить**.

   Активный лист будет скопирован.

Удаление активного листа

Чтобы удалить активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Активные листы**.
2. Установите флажки рядом с активными листами, которые вы хотите удалить.
   Если вы хотите удалить все листы, установите флажок рядом со столбцом **Название**.

   > Должен быть установлен хотя бы один флажок.

3. Нажмите на кнопку **Удалить**.
4. Нажмите на кнопку **OK**.

   Активные листы будут удалены.

Просмотр записей в активном листе

Чтобы просмотреть список записей в активном листе:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

Откроется таблица записей для выбранного листа.

Таблица содержит следующие данные:

- **Ключ** – значение ключа записи.
- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте активных листов в KUMA.
- **Срок действия** – дата и время, когда запись должна быть удалена.

  Если при создании активного листа в поле **Срок жизни** было указано значение 0, записи этого активного листа хранятся 36000 дней (около 100 лет).
- **Создано** – время создания активного листа.
- **Последнее обновление** – время последнего обновления активного листа.

Поиск записей в активном листе

Чтобы найти запись в активном листе:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. В поле **Поиск** введите значение ключа записи или несколько знаков из ее ключа.

В таблице записей активного листа отобразятся только те записи, в ключе которых есть введенные символы.

Добавление записи в активный лист

Чтобы добавить запись в активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. Установите флажок напротив нужного коррелятора.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Создать запись**.

7. Укажите значения для следующих параметров:

   a. В поле **Ключ** введите имя записи.

      Вы можете указать несколько значений, используя символ "|".

      > Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

   b. В поле **Значение** укажите значения для полей в столбце **Поле**.

      KUMA берет названия полей из корреляционных правил, к которым привязан активный лист. Эти названия недоступны для редактирования. Вы можете удалить эти поля при необходимости.

   c. Если вы хотите добавить дополнительное значение, нажмите на кнопку **Добавить элемент**.

   d. В столбце **Поле** укажите название поля.

      Название должно соответствовать следующим требованиям:

      - Название уникально.
      - Не содержит табуляцию.
      - Не содержит специальные символы, кроме символа нижнего подчеркивания.
      - Максимальное количество символов – 128.

        > Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.

   e. В столбце **Значение** укажите значение для этого поля.

      Оно должно соответствовать следующим требованиям:

      - Не содержит табуляцию.
      - Не содержит специальные символы, кроме символа нижнего подчеркивания.
      - Максимальное количество символов – 1024.

      Поле не является обязательным.

8. Нажмите на кнопку **Сохранить**.

Запись добавлена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Дублирование записей в активном листе

Чтобы дублировать запись в активном листе:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Установите флажок для записи, которую вы хотите скопировать.
7. Нажмите на кнопку **Дублировать**.
8. Укажите нужные вам параметры.

   Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

   Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.
9. Нажмите на кнопку **Сохранить**.

Запись будет скопирована. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Изменение записи в активном листе

Чтобы изменить запись в активном листе:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.

6. Нажмите на название записи в столбце **Ключ**.

7. Укажите требуемые значения.

8. Нажмите на кнопку **Сохранить**.

Запись будет изменена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Ограничения, действующие при редактировании записи:

- Название записи недоступно для редактирования. Вы можете изменить его, выполнив импорт аналогичных данных с другим названием.
- Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.
- Значения в столбце **Значение** должны соответствовать следующим требованиям:
  - Не содержит буквы русского алфавита.
  - Не содержит пробелы и табуляцию.
  - Не содержит специальные символы, кроме символа нижнего подчеркивания.
  - Максимальное количество символов – 128.

Удаление записей в активном листе

Чтобы удалить записи из активного листа:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.

6. Установите флажки для записей, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

Должен быть установлен хотя бы один флажок.

7. Нажмите на кнопку **Удалить**.

8. Нажмите на кнопку **OK**.

Записи будут удалены.

Импорт данных в активный лист

Чтобы импортировать данные в активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. Наведите курсор мыши на строку с требуемым активным листом.

6. Нажмите на ... слева от названия активного листа.

7. Выберите **Импортировать**.

   Откроется окно импорта активного листа.

8. В поле **Файл** выберите файл, который требуется импортировать.

9. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**
   - **tsv**
   - **internal**

10. В поле **Ключевое поле** введите название столбца с ключами записей активного листа.

11. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в активный лист. Записи, внесенные в лист ранее, сохраняются.

При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в виджетах, при наличии недопустимых символов в данных виджеты будут отображаться некорректно.

Экспорт данных из активного листа

Чтобы экспортировать активный лист:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. Наведите курсор мыши на строку с требуемым активным листом.
6. Нажмите на ... слева от нужного активного листа.
7. Нажмите на кнопку **Экспортировать**.

Активный лист будет загружен в формате JSON с использованием настроек вашего браузера. Название загруженного файла соответствует названию активного листа.

Предустановленные активные листы

В поставку OSMP включены перечисленные в таблице ниже активные листы.

Предустановленные активные листы

Имя активного листа	Описание
[OOTB][AD] End-users tech support accounts	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Successful authentication with same user account on multiple hosts. В активный список могут быть добавлены учетные записи сотрудников технической поддержки. Записи не удаляются из активного списка.
[OOTB][AD] List of requested TGT. EventID 4768	Активный список наполняется правилом [OOTB][AD][Technical] 4768. TGT Requested, также данный активный список используется в селекторе правила [OOTB][AD] Granted TGS without TGT (Golden Ticket). Записи удаляются из списка через 10 часов после внесения.
[OOTB][AD] List of sensitive groups	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Membership of sensitive group was modified. В активный список могут быть добавлены критичные доменные группы, членство в которых необходимо отслеживать. Записи не удаляются из активного списка.
[OOTB][Linux] CompromisedHosts	Активный список наполняется правилом [OOTB] Successful Bruteforce потенциально скомпрометированными устройствами под управлением операционной системой Linux. Записи удаляются из списка через 24 часов после внесения.

Словари

Описание параметров

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами KUMA.

Словари могут использоваться в следующих сервисах и функциях KUMA:

- Коллектор.
- Правила корреляции.
- Нормализаторы.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.
- **Тип** (обязательно) – тип словаря. От выбранного типа зависит формат данных, которые может содержать словарь:
  - В тип **Словарь** можно добавлять пары ключ–значение.

    Не рекомендуется добавлять в словари этого типа более 50 000 записей.

    > При добавлении в словарь строк с одинаковыми ключами каждая новая строка будет записана поверх уже существующий строки с тем же самым ключом. В итоге в словарь будет добавлена только одна строка.

  - В тип **Таблица** можно добавлять данные в виде сложных таблиц. С этим типом словарей можно взаимодействовать с помощью REST API.
- Блок параметров **Значения** – содержит таблицу с данными словаря:

  Для типа **Словарь** в блоке отображается перечень пар **Ключ** – **Значение**. Вы можете нажать на кнопку +, чтобы добавить строки в таблицу. Вы можете удалить строки с помощью на кнопки ×, которая отображается при наведении курсора мыши на нужную строку. В поле **Ключ** допустимо указать уникальное значение: максимум 128 символов Юникода, первый символ не может быть $. В поле **Значение** допустимо указать значение: максимум 255 символов Юникода, первый символ не может быть $. Допускается добавить одну или несколько пар **Ключ** – **Значение**.

  - Для типа **Таблица** в блоке отображается таблица с данными. Вы можете нажать на кнопку +, чтобы добавить строки или столбцы в таблицу. Удалить строки и столбцы можно, нажав на кнопки ×, которые отображаются при наведении курсора мыши на нужную строку или заголовок нужного столбца. Заголовки столбцов доступны для редактирования.

  Если словарь содержит больше 5000 записей, они не отображаются в Консоли KUMA. Для просмотра содержимого таких словарей содержимое необходимо экспортировать в формат CSV. Если CSV-файл отредактировать и снова импортировать в KUMA, словарь будет обновлен.

Импорт и экспорт словарей

Вы можете импортировать или экспортировать данные словарей в формате CSV (в кодировке UTF-8) с помощью кнопок **Импортировать CSV** и **Экспортировать CSV**.

Формат CSV-файла зависит от типа словаря:

- Тип **Словарь**:

  `{КЛЮЧ},{ЗНАЧЕНИЕ}\n`

- Тип **Таблица**:

  `{Заголовок столбца 1},{Заголовок столбца N},{Заголовок столбца N+1}\n`

  `{Ключ1},{ЗначениеN},{ЗначениеN+1}\n`

  `{Ключ2},{ЗначениеN},{ЗначениеN+1}\n`

  Ключи должны быть уникальными как для CSV-файла, так и для словаря. В таблицах ключи указываются в первом столбце. Ключ должен содержать от 1 до 128 символов Юникода.

  Значения должны содержать от нуля до 256 символов Юникода.

При импорте содержимое словаря перезаписывается загружаемым файлом. При импорте в словарь также изменяется название ресурса, чтобы отразить имя импортированного файла.

При экспорте, если ключ или значение содержат символы запятой или кавычек (, и "), они заключаются в кавычки ("). Также символ кавычки (") экранируется дополнительной кавычкой (").

Если в импортируемом файле обнаружены некорректные строки (например, неверные разделители), то при импорте в словарь такие строки будут проигнорированы, а при импорте в таблицу процесс импорта будет прерван.

Взаимодействие со словарями через API

Вы можете использовать REST API для чтения содержимого словарей **табличного типа**. Вы также можете изменить их, даже если эти ресурсы используются активными сервисами. Это позволяет, например, настроить обогащение событий данными из динамически изменяемых таблиц, выгружаемых из сторонних приложений.

Предустановленные словари

В поставку OSMP включены перечисленные в таблице ниже словари.

Предустановленные словари

Название словаря	Тип.	Описание
[OOTB] Ahnlab. Уровень важности	dictionary	Содержит таблицу соответствия между идентификатором приоритета и его названием.
[OOTB] Ahnlab. SeverityOperational	dictionary	Содержит значения параметра SeverityOperational и соответствующее ему описание.
[OOTB] Ahnlab. VendorAction	dictionary	Содержит таблицу соответствия между идентификатором выполняемой операции и ее названием.
[OOTB] Cisco ISE Message Codes	dictionary	Содержит коды событий Cisco ISE и соответствующие им имена.
[OOTB] DNS. Opcodes	dictionary	Содержит таблицу соответствия между десятичными кодами операций DNS и их описаниями, зарегистрированными IANA.
[OOTB] IANAProtocolNumbers	dictionary	Содержит номера портов транспортных протоколов (TCP, UDP) и соответствующие им имена сервисов, зарегистрированные IANA.

[OOTB] Juniper - JUNOS	dictionary	Содержит идентификаторы событий JUNOS и соответствующие им описания.
[OOTB] KEDR. AccountType	dictionary	Содержит идентификатор типа учетной записи и соответствующее ему наименование типа.
[OOTB] KEDR. FileAttributes	dictionary	Содержит идентификаторы атрибутов файлов, хранимые файловой системой, и соответствующие им описания.
[OOTB] KEDR. FileOperationType	dictionary	Содержит идентификаторы операций с файлами из API KATA и соответствующие им названия операции.
[OOTB] KEDR. FileType	dictionary	Содержит идентификаторы измененного файла из API KATA и соответствующие им описания типов файлов.
[OOTB] KEDR. IntegrityLevel	dictionary	Содержит SID параметра INTEGRITY LEVEL операционной системы Microsoft Windows и соответствующие им описания.
[OOTB] KEDR. RegistryOperationType	dictionary	Содержит идентификаторы операций с реестром из API KATA и соответствующие им значения.
[OOTB] Linux. Sycall types	dictionary	Содержит идентификаторы системных вызовов ОС Linux и соответствующие им названия.
[OOTB] MariaDB Error Codes	dictionary	Словарь содержит коды ошибок СУБД MariaDB и используется нормализатором [OOTB] MariaDB Audit Plugin syslog для обогащения событий.
[OOTB] Microsoft SQL Server codes	dictionary	Содержит идентификаторы ошибок MS SQL Server и соответствующие им описания.
[OOTB] MS DHCP Event IDs Description	dictionary	Содержит идентификаторы событий DHCP сервера Microsoft Windows и соответствующие им описания.
[OOTB] S-Terra. Dictionary MSG ID to Name	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им имена событий.
[OOTB] S-Terra. MSG_ID to Severity	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им значения Severity.
[OOTB] Syslog Priority To Facility and Severity	table	Таблица содержит значения **Приоритет** и соответствующие ему значения полей **Facility and Severity**.
[OOTB] VipNet Coordinator syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления, и соответствующие им значения.
[OOTB] Wallix EventClassId - DeviceAction	dictionary	Содержит идентификаторы событий Wallix AdminBastion и соответствующие им описания.
[OOTB] Windows.Codes (4738)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4738, и соответствующие им имена.
[OOTB] Windows.Codes (4719)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4719, и соответствующие им имена.
[OOTB] Windows.Codes (4663)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4663, и соответствующие им имена.
[OOTB] Windows.Codes (4662)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4662, и соответствующие им имена.
[OOTB] Windows. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий ОС Windows и соответствующие имена событий.
[OOTB] Windows. FailureCodes (4625)	dictionary	Содержит идентификаторы из полей **Failure Information\Status** и **Failure Information\Sub Status** события 4625 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. ImpersonationLevels (4624)	dictionary	Содержит идентификаторы из поля **Impersonation level** событий с идентификатором 4624 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. KRB ResultCodes	dictionary	Содержит коды ошибок Kerberos v5 и соответствующие им описания.
[OOTB] Windows. LogonTypes (Windows all events)	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.
[OOTB] Windows_Terminal Server. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий Microsoft Terminal Server и соответствующие им имена.
[OOTB] Windows. Validate Cred. Error Codes	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.

[OOTB] ViPNet Coordinator Syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления, и соответствующие им значения.
[OOTB] Syslog Priority To Facility and Severity	table	Содержит значения Priority и соответствующие ему значения полей Facility and Severity.

Правила реагирования

Правила реагирования запускают для заданных событий автоматическое выполнение задач Kaspersky Security Center, действия по реагированию для Kaspersky Endpoint Detection and Response, KICS for Networks, Active Directory и запуск пользовательского скрипта.

Автоматическое выполнение задач Kaspersky Security Center, Kaspersky Endpoint Detection and Response, KICS for Networks и Active Directory по правилам реагирования доступно при интеграции с перечисленными приложениями.

Вы можете настроить правила реагирования в разделе **Мониторинг** → **Ресурсы** → **Правила реагирования**, а затем выбрать созданное правило реагирования в раскрывающемся списке в параметрах коррелятора. Также можно настроить правила реагирования прямо в настройках коррелятора.

Правила реагирования для Kaspersky Security Center

Вы можете настроить правила реагирования для автоматического запуска задач антивирусной проверки и обновления на активах Kaspersky Security Center.

При создании и изменении правил реагирования для Kaspersky Security Center вам требуется задать значения для следующих параметров.

Вкладка Общие

Параметры правила реагирования

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип.	Обязательный параметр, доступен при интеграции KUMA с Kaspersky Security Center. Правила реагирования **osmptasks**.
Задаче Open Single Management Platform	Обязательный параметр. Название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, их названия должны начинаться со слова "`KUMA`". Например, `KUMA antivirus check` (без учета регистра и без кавычек). С помощью KUMA можно запустить следующие типы задач Kaspersky Security Center: • Обновление. • Поиск вирусов.

Параметр	Описание
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения: • SourceAssetID • DestinationAssetID • DeviceAssetID
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание правила реагирования. Вы можете добавить до 4000 символов Юникода.

Параметр	Описание
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если правила реагирования принадлежат общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от Сервера Kaspersky Security Center, к которому подключен главный тенант.

Если в правиле реагирования выбрана задача, которая отсутствует на Сервере администрирования Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к корреляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **OK**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь между правилом реагирования и сервисом. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила реагирования для пользовательского скрипта

Вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий, и настроить правила реагирования для автоматического запуска этого скрипта. В этом случае приложение запустит скрипт при получении событий, соответствующих правилам реагирования.

Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

При создании и изменении правил реагирования для произвольного скрипта вам требуется задать значения для следующих параметров.

Вкладка Общие

Параметры правила реагирования

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип.	Обязательный параметр. Тип правила реагирования, **script**.
Время ожидания	Количество секунд, в течение которого должно завершиться выполнение скрипта. Если это время превышено, выполнение скрипта прерывается.
Название скрипта	Обязательный параметр. Имя файла скрипта. Если ресурс реагирования прикреплен к сервису коррелятора, но в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
Аргументы скрипта	Параметры или значения полей событий, которые необходимо передать скрипту. Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь. Параметры можно обрамлять кавычками ("). Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт. Пример: `-n "\"usr\": {{.SourceUserName}}"`
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов Юникода.

Параметр	Описание
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к корреляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **OK**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь между правилом реагирования и сервисом. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила реагирования для KICS for Networks

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

При создании и изменении правил реагирования для KICS for Networks вам требуется задать значения для следующих параметров.

Вкладка Общие

Параметры правила реагирования

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип.	Обязательный параметр. Тип правила реагирования, **kics**.
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно выполнить действия по реагированию. Возможные значения: • SourceAssetID • DestinationAssetID • DeviceAssetID

Параметр	Описание
Задача KICS for Networks	Действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию: • **Изменить статус актива на Разрешенное**. • **Изменить статус актива на Неразрешенное**. При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов Юникода.

Параметр	Описание
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к корреляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **OK**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь между правилом реагирования и сервисом. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила реагирования для Kaspersky Endpoint Detection and Response

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах Kaspersky Endpoint Detection and Response. Например, вы можете настроить автоматическую изоляцию актива от сети.

При создании и изменении правил реагирования для Kaspersky Endpoint Detection and Response вам требуется задать значения для следующих параметров.

Вкладка Общие

Параметры правила реагирования

Параметр	Описание
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно выполнить действия по реагированию. Возможные значения: • SourceAssetID • DestinationAssetID • DeviceAssetID

Параметр	Описание

Тип задач	Действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
	• Включить сетевую изоляцию. При выборе этого типа реагирования вам нужно задать значения для параметра:
	  • **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов. При необходимости вы можете **добавить исключение для сетевой изоляции**.
	  Чтобы добавить исключение для сетевой изоляции:
	  a. Нажмите на кнопку **Добавить исключение**.
	  b. Выберите направление сетевого трафика, которое не должно быть заблокировано:
	  • Входящее.
	  • Исходящее.
	  • Входящее/Исходящее.
	  c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.
	  d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.
	  e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.
	  f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.
	  При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность приложения. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.
	• Выключить сетевую изоляцию.
	• Добавить правило запрета. При выборе этого типа реагирования вам нужно задать значения для следующих параметров:
	  • **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, выполнение которых требуется запретить.
	  Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в распространяемые поля правила корреляции.
	  • **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.
	  Хотя бы одно из указанных выше полей должно быть заполнено.
	• Удалить правило запрета.
	• Запустить приложение. При выборе этого типа реагирования вам нужно задать значения для следующих параметров:
	  • **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
	  • **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
	  • **Текущая директория** – директория, в которой на момент запуска располагается файл.
	  При срабатывании правила реагирования для пользователей с ролью Главный администратор в разделе **Диспетчер задач** консоли приложения отобразится задача **Запустить приложение**. В столбце Создал **таблицы задач** для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.
	Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск приложения.
	На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.

Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание правила реагирования. Вы можете добавить до 4000 символов Юникода.

Параметр	Описание
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к корреляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **OK**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь между правилом реагирования и сервисом. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила реагирования через Active Directory

Правила реагирования через Active Directory определяют действия, которые будут применяться к учетной записи в случае срабатывания правила.

При создании и изменении правил реагирования через Active Directory вам требуется задать значения для следующих параметров.

Вкладка Общие

Параметры правила реагирования

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип.	Обязательный параметр. Тип правила реагирования, **Реагирование через Active Directory**.
Источник идентификатора аккаунта	Поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения: • SourceAccountID • DestinationAccountID

Параметр	Описание
Команда Active Directory	Команда, которая будет применяться к учетной записи при срабатывании правила реагирования. Доступные значения: • **Добавить учетную запись в группу** Группа Active Directory, из которой или в которую требуется переместить учетную запись. В обязательном поле **Отличительное имя** необходимо указать полный путь к группе. Например, CN = Team, OU = Groups, OU = ExchangeObjects, DC = example, DC = com. В рамках одной операции можно указать только одну группу. • **Удалить учетную запись из группы** Группа Active Directory, из которой или в которую требуется переместить учетную запись. В обязательном поле **Отличительное имя** необходимо указать полный путь к группе. Например, CN = Team, OU = Groups, OU = ExchangeObjects, DC = example, DC = com. В рамках одной операции можно указать только одну группу. • Сбросить пароль учетной записи Если в вашем домене Active Directory для учетных записей допускается установка флажка **User cannot change password**, использование в качестве реагирования сброса пароля учетной записи приведет к коллизии требований к учетной записи: пользователь не сможет аутентифицироваться. Администратору домена потребуется снять один из флажков для затронутой учетной записи: **User cannot change password** или **User must change password at next logon**. • Блокировать учетную запись

Параметр	Описание
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или создать фильтр. **Создание фильтра в ресурсах** Все поля события KUMA имеют значение по умолчанию. Для всех числовых полей это значение равно 0. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. В этом случае вы сможете использовать созданный фильтр в разных сервисах. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. В блоке параметров **Условия** укажите условия, которым должны соответствовать события: a. Нажмите на кнопку **Добавить условие**. b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска. В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров для определения значения, которое будет передано в фильтр. Например, при выборе значения **активный лист** вам нужно указать название активного листа, ключ записи и поле ключа записи. c. В раскрывающемся списке **Оператор** выберите оператор. **Операторы фильтров** • **=** – левый операнд равен правому операнду. • **<** – левый операнд меньше правого операнда. • **<=** – левый операнд меньше или равен правому операнду. • **>** – левый операнд больше правого операнда. • **>=** – левый операнд больше или равен правому операнду. • **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети). • **contains** – левый операнд содержит значения правого операнда. • **startsWith** – левый операнд начинается с одного из значений правого операнда. • **endsWith** – левый операнд заканчивается одним из значений правого операнда. • **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2. • **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке). Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка. Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`. • **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде. Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии. • **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов. • **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события. • **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда. • **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде. • **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах. • **inContextTable** – присутствует ли в указанной контекстной таблице запись. • **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Параметр	Описание
	d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят. e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. Вы можете добавить несколько условий или группу условий. 5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**. 6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку ↗.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к корреляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **OK**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете удалить связь между правилом реагирования и сервисом. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила сбора и анализа данных

Правила сбора и анализа данных используются для обнаружения инцидентов путем анализа событий, сохраненных в базе данных OSMP.

В отличие от потоковой корреляции и запуска ретроспективной проверки, правила сбора и анализа данных предусматривают предварительную обработку данных с помощью SQL-запросов (в том числе выполнение дополнительных вычислений, группировку и агрегацию через SQL) и регулярный запуск по расписанию. При наличии корректно настроенных правил сбора и анализа данных SIEM может помочь вам в обнаружении сложных атак.

> Для работы с разделом вам необходимо иметь одну из следующих ролей: Главный администратор, Администратор тенанта, Аналитик первого уровня, Аналитик второго уровня.

При создании и изменении правил сбора и анализа данных требуется задать значения для параметров, указанных в таблице ниже.

Параметр	Описание
Имя	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс. Если у вас есть доступ только к одному тенанту, поле заполняется автоматически. Если у вас есть доступ к нескольким тенантам, подставляется название первого тенанта из списка доступных вам тенантов. Вы можете выбрать любой тенант из этого списка.
SQL	Обязательный параметр. SQL-запрос должен содержать функцию агрегации с ограничением LIMIT и/или группировку данных с ограничением LIMIT. Значение LIMIT должно быть от 1 до 10 000. Примеры SQL-запросов: • Запрос, содержащий только функцию агрегации: `SELECT count(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10` • Запрос, содержащий только группировку данных: `SELECT SourceAddress, DeviceCustomFloatingPoint1 FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10` • Запрос, содержащий функцию агрегации и группировку данных: `SELECT SourceAddress, sum(DeviceCustomFloatingPoint1) FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10` • Запрос, содержащий выражение из функций агрегации: `SELECT stddevPop(DeviceCustomFloatingPoint1) + avg(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
Частота запуска запроса	Обязательный параметр. Интервал выполнения SQL-запроса. Вы можете указать интервал в минутах, часах и днях. Минимальный интервал – 1 минута. Время ожидания ответа на SQL-запрос по умолчанию равно интервалу, который вы задаете в этом поле. Если выполнение SQL-запроса превышает время ожидания, возникает ошибка. В этом случае рекомендуется увеличить интервал. Например, если значение интервала равно 1 минуте, при этом запрос выполняется 80 секунд, то рекомендуется увеличить значение интервала как минимум до 90 секунд.
Теги	Необязательный параметр. Теги для поиска ресурса.
Глубина	Необязательный параметр. Выражение для определения нижней границы интервала поиска событий в базе данных. Чтобы выбрать значение из списка либо задать глубину в формате относительного интервала, установите курсор в поле. Например, если вы хотите находить все события за период, прошедший с текущего момента назад на один час, установите относительный интервал now-1h.
Описание	Необязательный параметр. Описание правила сбора и анализа данных.
Сопоставление	Параметры для настройки сопоставления полей результата SQL-запроса с событиями KUMA: **Исходное поле** – поле результата SQL-запроса, которое вы хотите преобразовать в событие KUMA. **Поле события** – поле события KUMA. Вы можете выбрать одно из доступных значений в списке, установив курсор мыши в это поле. **Подпись** – уникальная пользовательская метка полей событий, которые начинаются с `DeviceCustom*`. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить сопоставление**. Для удаления строки установите флажок рядом с нужной строкой и нажмите на кнопку 🗑. Если вы не хотите заполнять поля вручную, вы можете нажать на кнопку **Обновить сопоставление из SQL**. Значения полей SQL запроса, включая псевдонимы (при наличии), подставятся в таблицу сопоставления полей. Например, если поле в SQL-запросе имеет значение `SourceAddress` и это значение совпадает с названием поля события, это значение проставляется в столбце **Поле события** в таблице сопоставления полей. При повторном нажатии на кнопку **Обновить сопоставление из SQL** таблица не обновляется, а значения полей SQL-запроса добавляются в нее повторно.

Вы можете создавать правило сбора и анализа данных одним из следующих способов:

- В разделе **Мониторинг** → **Ресурсы и сервисы** → **Правила сбора и анализа данных**.

1. В разделе **Мониторинг** → **Поиск угроз**.

*Чтобы создать правило сбора и анализа данных в разделе **Поиск угроз**:*

1. Создайте или сгенерируйте SQL-запрос и нажмите кнопку **Создать правило сбора и анализа данных**.

   В браузере откроется новая вкладка создания правила сбора и анализа данных с предзаполненными полями **SQL запрос** и **Глубина**. Таблица сопоставления полей также будет заполнена автоматически, если в SQL-запросе вы не использовали звездочку (*).

2. Заполните обязательные поля.

   Если необходимо, вы можете изменить значение в поле **Частота выполнения SQL-запроса**.

3. Сохраните параметры.

Правило сбора и анализа данных сохранено и доступно в разделе **Мониторинг** → **Ресурсы и сервисы** → **Правила сбора и анализа данных**. Чтобы правило сбора и анализа данных выполнялось, вам нужно создать для него расписание.

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Kaspersky EDR Expert, предназначенный для управления антивирусной защитой сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.

- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.

- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.

- Для удаленной установки приложения "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.

- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.

- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky EDR Expert перезапускает главный Сервер администрирования и все виртуальные Серверы.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Коннекторы

Коннекторы используются для установки соединений между сервисами KUMA, активного и пассивного получения событий.

В приложении доступны следующие типы коннекторов:

- tcp – используется для пассивного получения событий по протоколу TCP.
- udp – используется для пассивного получения событий по протоколу UDP.
- netflow – используется для пассивного получения событий в формате NetFlow.
- sflow – используется для пассивного получения событий в формате SFlow.
- nats-jetstream – используется для взаимодействия с брокером сообщений NATS.
- kafka – используется для коммуникации с шиной данных Apache Kafka.
- http – используется для получения событий по протоколу HTTP.
- sql – используется для выборки данных из СУБД.

  Приложение поддерживает работу со следующими типами баз данных SQL:

  - SQLite.
  - MSSQL.
  - MySQL.
  - PostgreSQL.
  - Cockroach.
  - Oracle.
  - Firebird.
  - ClickHouse.
- file – используется для получения данных из текстового файла.
- 1c-log и 1c-xml – используются для получения данных из журналов 1С.

- diode – используется для однонаправленной передачи данных в промышленных ICS-сетях с использованием диодов данных.
- ftp – используется для получения данных по протоколу File Transfer Protocol.
- sftp – используется для получения данных по протоколу Secure File Transfer Protocol.
- nfs – используется для получения данных по протоколу Network File System.
- wmi – используется для получения данных с помощью Windows Management Instrumentation.
- wec – используется для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС устройства под управлением Windows.
- snmp – используется для получения данных с помощью Simple Network Management Protocol.
- snmp-trap – используется для получения данных с помощью "ловушек" Simple Network Management Protocol (SNMP Trap).
- kata/edr – используется для получения данных KEDR по API.
- vmware – используется для получения данных VMware vCenter по API.
- elastic – используется для получения данных Elasticsearch.
- etw – используется для получения расширенных журналов событий DNS-сервера.
- universalAPI – используются для получения данных из любых REST API, поддерживающих ответы в формате JSON. Поддерживается фильтрация по уникальному идентификатору и режим итераций.
- smb – используется для получения данных по протоколу SMB (Server Message Block).
- http-streaming – используется для потокового получения событий по протоколу HTTP. Коннектор обрабатывает тело запроса по частям, что позволяет снизить потребление памяти.

Просмотр параметров коннектора

Чтобы просмотреть параметры коннектора:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Коннекторы**.
2. В структуре папок выберите папку, в которой располагается нужный вам коннектор.
3. Выберите коннектор, параметры которого вы хотите просмотреть.

Параметры коннекторов отображаются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Подробное описание параметров каждого коннектора см. в разделе *Параметры коннекторов*.

Добавление коннектора

Вы можете включить отображение непечатаемых символов для всех полей ввода, кроме поля **Описание**.

Чтобы добавить коннектор:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Коннекторы**.

2. В структуре папок выберите папку, в которой должен располагаться коннектор.

   > Корневые папки соответствуют тенантам. Для того, чтобы коннектор был доступен определенному тенанту, его следует создать в папке этого тенанта.

   Если в дереве папок отсутствует требуемая папка, вам нужно создать ее.

   По умолчанию добавляемые коннекторы создаются в папке **Общий**.

3. Нажмите на кнопку **Добавить коннектор**.

4. Укажите параметры для выбранного типа коннектора.

   Параметры, которые требуется указать для каждого типа коннектора, приведены в разделе *Параметры коннекторов*.

5. Нажмите на кнопку **Сохранить**.

Параметры коннекторов

Этот раздел содержит описание параметров всех поддерживаемых KUMA типов коннекторов.

Тип kata/edr

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип коннектора, **kata/edr**.

- **URL** (обязательно) – URL, по которому доступно получение телеметрии с сервера KATA/EDR. В URL указывается устройство и порт, по умолчанию порт 443. Если KATA/EDR развернута в кластере, можно указать несколько URL, чтобы обеспечить высокую доступность подключения.

- **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения к серверу KATA/EDR. Вы можете выбрать ресурс секрета в раскрывающемся списке или создать его, нажав на значок плюса (+). При создании секрета вы можете указать пользовательский сертификат и закрытый ключ или автоматически сгенерировать новый самоподписанный сертификат и закрытый ключ. Выбранный секрет можно изменить, нажав на значок карандаша ( ).

- **Внешний ID** – идентификатор для внешних систем. KUMA генерирует идентификатор и заполняет это поле автоматически.

- **Описание** – описание ресурса: до 4000 символов Юникода.

Вкладка **Дополнительные параметры**:

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- **Кодировка символов** – параметр исходной кодировки символов для конвертации в UTF-8. Рекомендуется применять конвертацию только в том случае, если в полях нормализованного события отображаются недопустимые символы. Значение по умолчанию – не выбрано.

- **Максимальное количество событий** – максимальное количество событий в одном запросе. По умолчанию используется значение, заданное на сервере KATA/EDR.

- **Время ожидания получения событий** – время ожидания получения событий от сервера KATA/EDR в секундах. По умолчанию указано значение 0 – это означает, что используется значение, заданное на сервере KATA/EDR.

- **Время ожидания ответа** – время ожидания ответа от сервера KATA/EDR в секундах. Значение по умолчанию: 1800 сек, отображается как 0.

- **Фильтр KEDRQL** – фильтр запросов к серверу KATA/EDR. Подробнее о языке запросов см. в Справке KEDR.

Секреты

Секреты используются для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые должны использоваться KUMA для взаимодействия с внешними службами. Если секрет хранит данные учетной записи, такие как логин и пароль, то при подключении коллектора к источнику событий учетная запись пользователя, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

Секреты можно использовать в следующих сервисах и функциях KUMA:

- Коллектор (при использовании шифрования TLS).

- Коннектор (при использовании шифрования TLS).

- Точки назначения (при использовании шифрования TLS или авторизации).

- Прокси-серверы.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип секрета.

  При выборе в раскрывающемся списке типа секрета отображаются параметры для настройки выбранного типа секрета. Эти параметры описаны ниже.

- **Описание** – вы можете добавить до 4000 символов Юникода.

В зависимости от типа секрета доступны различные поля для заполнения. Вы можете выбрать один из следующих типов секрета:

- **credentials** – тип секрета используется для хранения данных учетных записей, с помощью которых осуществляется подключение к внешним службам, например к SMTP-серверам. При выборе этого типа секрета требуется заполнить поля **Пользователь** и **Пароль**. При использовании в ресурсе **Секрет** типа credentials для подключения коллектора к источнику событий, например СУБД, учетная запись пользователя, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

  При изменении ранее сохраненного секрета типа credentials поля с именем пользователя и паролем отображаются пустыми. Значения этих полей сохранены, вам не нужно вводить их повторно.

- **token** – тип секрета используется для хранения токенов для API-запросов. Токены используются, например, при подключении к IRP-системам. При выборе этого типа секрета требуется заполнить поле **Токен**.

- **ktl** – тип секрета используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Пользователь** и **Пароль** (обязательные поля) – имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – позволяет загрузить ключ сертификата Kaspersky Threat Intelligence Portal.

  - **Пароль PFX-файла** (обязательно) – пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.

- **urls** – тип секрета используется для хранения URL для подключения к базам SQL и прокси-серверам. В поле **Описание** требуется описать, для какого именно подключения вы используете секрет **urls**.

  Вы можете указать URL в следующих форматах: hostname:port, IPv4:port, IPv6:port, :port.

- **pfx** – тип секрета используется для импорта PFX-файла с сертификатами. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – используется для загрузки PFX-файла. Файл должен содержать сертификат и ключ. В PFX-файлы можно включать сертификаты, подписанными центрами сертификации, для проверки сертификатов сервера.

  - **Пароль PFX-файла** (обязательно) – используется для ввода пароля для доступа к ключу сертификата.

- **kata/edr** – тип секрета используется для хранения файла сертификата и закрытого ключа, требуемых при подключении к серверу Kaspersky Endpoint Detection and Response. При выборе этого типа секрета вам требуется загрузить следующие файлы:

  - Файл сертификата – сертификат сервера KUMA.

    Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.

  - Закрытый ключ шифрования соединения – RSA-ключ сервера KUMA.

Ключ должен быть без пароля и с заголовком PRIVATE KEY. Вы можете загрузить только один файл ключа.

Вы можете сгенерировать файлы сертификата и ключа по кнопке ⭳.

- **snmpV1** – тип секрета используется для хранения значения **Уровень доступа** (например, `public` или `private`), которое требуется при взаимодействии по протоколу Simple Network Management Protocol.
- **snmpV3** – тип секрета используется для хранения данных, требуемых при взаимодействии по протоколу Simple Network Management Protocol. При выборе этого типа секрета требуется заполнить следующие поля:
  - **Пользователь** – имя пользователя, указывается без домена.
  - **Уровень безопасности** – уровень безопасности пользователя:
    - **NoAuthNoPriv** – сообщения отправляются без аутентификации и без обеспечения конфиденциальности.
    - **AuthNoPriv** – сообщения посылаются с аутентификацией, но без обеспечения конфиденциальности.
    - **AuthPriv** – сообщения посылаются с аутентификацией и обеспечением конфиденциальности.

    В зависимости от выбранного уровня могут отобразиться дополнительные параметры.
  - **Пароль** – пароль аутентификации пользователя SNMP. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
  - **Протокол аутентификации** – доступны следующие протоколы: MD5, SHA, SHA224, SHA256, SHA384, SHA512. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
  - **Протокол шифрования** – протокол, используемый для шифрования сообщений. Доступны следующие протоколы: DES, AES. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.
  - **Пароль обеспечения безопасности** – пароль шифрования, который был указан при создании пользователя SNMP. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.
- **certificate** – тип секрета используется для хранения файлов сертификатов. Файлы загружаются в ресурс с помощью кнопки **Загрузить файл сертификата**. Поддерживаются открытые ключи сертификата X.509 в Base64.
- **ssh private key** – этот тип секрета используется в коннекторе SFTP для подключения к SFTP-серверу. Если вы выбрали этот тип секрета, вам нужно указать имя пользователя и файл, содержащий закрытый SSH-ключ.

Предустановленные секреты

В поставку OSMP включены перечисленные в таблице ниже секреты.

Название секрета	Описание
[OOTB] Continent SQL connection	Хранит конфиденциальные данные и параметры подключения к БД АПКШ Континент. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MSSQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MySQL Connection	Хранит конфиденциальные данные и параметры подключения к БД MySQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.
[OOTB] Oracle Audit Trail SQL Connection	Хранит конфиденциальные данные и параметры подключения к БД Oracle. Для использования необходимо указать логин и пароль БД.
[OOTB] SecretNet SQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL системы SecretNet. Для использования необходимо указать логин и пароль БД.

Контекстные таблицы

Контекстная таблица – это контейнер для массива данных, которые используются корреляторами KUMA при анализе событий по правилам корреляции. Вы можете создавать контекстные таблицы в разделе **Мониторинг** →**Ресурсы**. Данные контекстной таблицы хранятся только в корреляторе, в который она была добавлена с помощью фильтров или действий в корреляционных правилах.

Вы можете наполнять контекстные таблицы автоматически с помощью корреляционных правил типа simple и operational или импортировать файл с данными для контекстной таблицы.

Вы можете добавлять, копировать и удалять контекстные таблицы, а также изменять их настройки.

Контекстные таблицы можно использовать в следующих сервисах и функциях KUMA:

- Правила корреляции.
- Панель мониторинга.

Одна и та же контекстная таблица может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными корреляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.

В контекстную таблицу добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, удалять, импортировать и экспортировать записи в контекстной таблице коррелятора.

В процессе корреляции при удалении записей из контекстных таблиц в корреляторах создаются служебные события. Эти события существуют только в корреляторах, они не перенаправляются в другие точки назначения. Служебные события отправляются на обработку правилами корреляции того коррелятора, где работает контекстная таблица. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы.

Поля служебных событий удаления записи из контекстной таблицы описаны ниже.

Поле события	Значение или комментарий
ID	Идентификатор события.
Timestamp	Время удаления записи, срок жизни которой истек.
Имя	"context table record expired"
DeviceVendor	"Лаборатория Касперского".
DeviceProduct	"KUMA"
ServiceID	Идентификатор коррелятора.
ServiceName	Название коррелятора.
DeviceExternalID	Идентификатор контекстной таблицы.
DevicePayloadID	Ключ записи, срок жизни которой истек.
BaseEventCount	Увеличенное на единицу количество обновлений удаленной записи.
FileName	Название контекстной таблицы.
S.< поле контекстной таблицы > SA.< поле контекстной таблицы > N.< поле контекстной таблицы > NA.< поле контекстной таблицы > F.< поле контекстной таблицы > FA.< поле контекстной таблицы >	В зависимости от типа записи, выпавшей из контекстной таблицы, запись записывается в соответствующий тип события: Например, S.<поле контекстной таблицы> = <значение поля контекстной таблицы>. SA.<поле контекстной таблицы> = <массив значений поля контекстной таблицы> Записи контекстной таблицы логического типа имеют следующий формат: S.<поле контекстной таблицы> = true/false SA.<поле контекстной таблицы> = false,true,false

Просмотр списка контекстных таблиц

Чтобы просмотреть список контекстных таблиц коррелятора:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, для которого вы хотите просмотреть контекстные таблицы, выберите пункт **Смотреть контекстные таблицы**.

   Отобразится список **Контекстные таблицы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя контекстной таблицы.
- **Размер на диске** – размер контекстной таблицы.
- **Директория** – путь к контекстной таблице на сервере коррелятора KUMA.

Добавление контекстной таблицы

Чтобы добавить контекстную таблицу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Контекстные таблицы**.

2. В окне **Контекстные таблицы** нажмите на кнопку **Добавить**.

   Откроется окно **Создание контекстной таблицы**.

3. В поле **Название** введите имя контекстной таблицы.

4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

5. В поле **Срок жизни** укажите время, в течение которого в контекстной таблице будет храниться добавленная в него запись.

   По истечении указанного времени запись удаляется. Время указывается в секундах. Максимальное значение – `31536000` (1 год).

   Значение по умолчанию – `0`. Если в поле указано значение 0, время хранения записи неограниченно.

6. В поле **Описание** укажите любую дополнительную информацию.

   Вы можете использовать до 4000 символов Юникода.

   Поле не является обязательным.

7. В разделе **Схема** укажите состав полей контекстной таблицы и тип данных полей.

   В зависимости от типа данных поле может быть или не быть ключевым. Хотя бы одно поле в таблице должно быть ключевым полем. Имена всех полей должны быть уникальными.

   Для добавления строки таблицы нажмите на кнопку **Добавить** и заполните поля таблицы:

   a. В поле **Название** введите название поля. Максимальная длина – 128 символов.

   b. В раскрывающемся списке **Тип** выберите тип данных поля.

   Возможные типы данных поля

   Возможные типы данных поля контекстной таблицы

Тип данных поля	Может быть ключевым полем	Комментарий
Целое число	Да	—
Число с плавающей точкой	Да	—
Строка	Да	—
Логический оператор	Да	—
Timestamp	Да	Для поля этого типа проверяется, что значение поля больше или равно нулю. Другие операции не предусмотрены.
IP-адрес;	Да	Для поля этого типа проверяется, что значение поля соответствует формату IPv4, IPv6. Другие операции не предусмотрены.
Список целых чисел	Нет	—
Список чисел с плавающей точкой	Нет	—
Список строк	Нет	—

Тип данных поля	Может быть ключевым полем	Комментарий
Список логических типов	Нет	—
Список временных меток	Нет	Для поля этого типа проверяется, что каждый элемент списка больше или равен нулю. Другие операции не предусмотрены.
Список IP-адресов	Нет	Для поля этого типа проверяется, что каждый элемент списка соответствует формату IPv4, IPv6. Другие операции не предусмотрены.

c. Если вы хотите сделать поле ключевым, установите флажок **Ключевое поле**.

   В таблице может быть несколько ключевых полей. Ключевые поля задаются при создании контекстной таблицы, уникально идентифицируют запись таблицы и не могут изменяться.

   Если ключевых полей в контекстной таблице несколько, каждая запись таблицы уникально идентифицируется несколькими полями (составной ключ).

8. Добавьте нужное количество строк контекстной таблицы.

   После сохранения контекстной таблицы схему поменять нельзя.

9. Нажмите на кнопку **Сохранить**.

Контекстная таблица будет добавлена.

Просмотр параметров контекстной таблицы

Чтобы просмотреть параметры контекстной таблицы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Контекстные таблицы**.
2. В окне **Контекстные таблицы** в списке выберите контекстную таблицу, параметры которой вы хотите просмотреть.

Откроется окно с параметрами контекстной таблицы. В нем отображается следующая информация:

- **Название** – уникальное имя ресурса.
- **Тенант** – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Значение указывается в секундах.
- **Описание** – любая дополнительная информация о ресурсе.
- **Схема** – упорядоченный список полей и их типов данных с отметкой ключевых полей.

Изменение параметров контекстной таблицы

Чтобы изменить параметры контекстной таблицы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Контекстные таблицы**.

2. В окне **Контекстные таблицы** в списке выберите контекстную таблицу, параметры которой вы хотите изменить.

3. Укажите значения для следующих параметров:

   - **Название** – уникальное имя ресурса.

   - **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Значение указывается в секундах.

   - **Описание** – любая дополнительная информация о ресурсе.

   - **Схема** – упорядоченный список полей и их типов данных с отметкой ключевых полей. Если контекстная таблица не используется в корреляционном правиле, вы можете поменять состав полей.

     Если вы хотите изменить схему в контекстной таблице, которая уже используется в корреляционном правиле, выполните шаги инструкции ниже.

   Поле **Тенант** недоступно для редактирования.

4. Нажмите на кнопку **Сохранить**.

Чтобы изменить параметры контекстной таблицы, ранее используемой коррелятором:

1. Выполните экспорт данных из таблицы.

2. Скопируйте и сохраните путь к файлу с данными таблицы на диске коррелятора. Путь указан в столбце **Директория** в окне **Контекстные таблицы коррелятора**. Этот путь понадобится вам в дальнейшем для удаления файла с диска коррелятора.

3. Удалите из коррелятора контекстную таблицу.

4. Измените необходимые параметры контекстной таблицы.

5. Удалите файл с данными таблицы на диске коррелятора по пути из шага 2.

6. Добавьте в коррелятор контекстную таблицу, в которой вы изменили параметры.

7. Перезапустите коррелятор: в разделе **Ресурсы** → **Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором, в панели инструментов нажмите на значок с тремя точками и в открывшемся меню выберите **Перезапустить**.

8. Адаптируйте в экспортированной таблице (см. шаг 1) поля, чтобы они соответствовали полям таблицы, которую вы загрузили в коррелятор на шаге 6.

9. Импортируйте адаптированные данные в контекстную таблицу.

Дублирование параметров контекстной таблицы

Чтобы скопировать контекстную таблицу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Контекстные таблицы**.
2. Установите флажок рядом с контекстной таблицей, которую вы хотите копировать.
3. Нажмите на кнопку **Дублировать**.
4. Укажите нужные вам параметры.
5. Нажмите на кнопку **Сохранить**.

   Контекстная таблица будет скопирована.

Удаление контекстной таблицы

Вы можете удалить только те контекстные таблицы, которые не используются ни в одном в корреляторе.

Чтобы удалить контекстную таблицу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы** → **Контекстные таблицы**.
2. Установите флажки рядом с контекстными таблицами, которые вы хотите удалить.
   Если вы хотите удалить все контекстные таблицы, установите флажок рядом со столбцом **Название**.

   > Должен быть установлен хотя бы один флажок.

3. Нажмите на кнопку **Удалить**.
4. Нажмите на кнопку **OK**.

   Контекстные таблицы будут удалены.

Просмотр записей контекстной таблицы

Чтобы просмотреть список записей контекстной таблицы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. В контекстном меню коррелятора, контекстную таблицу которого вы хотите просмотреть, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. В столбце **Название** выберите нужную контекстную таблицу.

Откроется список записей для выбранной контекстной таблицы.

Список содержит следующие данные:

- **Ключ** – композитный ключ записи. Формируется из одного и более значений ключевых полей, разделенных символом "|". Если одно из значений ключевого поля отсутствует, то разделяющий символ все равно отображается.

  Например, ключ записи состоит из трех полей: `DestinationAddress`, `DestinationPort`, `SourceUserName`. При отсутствии значений в последних двух полях ключ записи будет отображаться следующим образом: `43.65.76.98| | `.

- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте контекстных таблиц в KUMA.

- **Срок действия** – дата и время, когда запись должна быть удалена.

  Если при создании контекстной таблицы в поле **Срок жизни** было указано значение 0, записи этой контекстной таблицы хранятся 36000 дней (около 100 лет).

- **Обновлено** – дата и время обновления контекстной таблицы.

Поиск записей в контекстной таблице

Чтобы найти запись в контекстной таблице:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите найти запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. В столбце **Название** выберите нужную вам контекстную таблицу.

   Откроется окно со списком записей для выбранной контекстной таблицы.

5. В поле **Поиск** введите значение ключа записи или несколько знаков из ее ключа.

В списке записей контекстной таблицы отобразятся только те записи, в ключе которых есть введенные символы.

Если под условие вашего поискового запроса попадают записи с пустыми значениями в ключе, в разделе **Панель мониторинга** на виджете отобразится текст <По вашему запросу ничего не найдено>. Рекомендуется уточнить условия поискового запроса.

Добавление записи в контекстную таблицу

Чтобы добавить запись в контекстную таблицу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите добавить запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.

5. Нажмите на кнопку **Добавить**.

   Откроется окно **Создать запись**.

6. В поле **Значение** укажите значения для полей в столбце **Поле**.

   KUMA берет названия полей из корреляционных правил, к которым привязана контекстная таблица. Эти названия недоступны для редактирования. Состав полей изменить невозможно.

   Если вы укажете не все значения полей, отсутствующие поля, включая ключевые, будут заполнены значениями по умолчанию. Из итоговой совокупности полей будет сформирован ключ записи, и запись будет добавлена в таблицу. Если такой ключ в таблице уже существует, отобразится ошибка.

   Список значений полей по умолчанию

Тип поля	Значение по умолчанию
Целое число	0
Число с плавающей точкой	0,0
Строка	""
Логический оператор	false
IP-адрес;	"0.0.0.0"
Timestamp	0
Список целых чисел	[]
Список чисел с плавающей точкой	[]
Список строк	[]
Список логических типов	[]
Список временных меток	[]
Список IP-адресов	[]

7. Нажмите на кнопку **Сохранить**.

Запись добавлена.

Изменение записи в контекстной таблице

Чтобы изменить запись в контекстной таблице:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, контекстную таблицу которого вы хотите изменить, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.
5. Нажмите на строку записи, которую вы хотите изменить.
6. Укажите требуемые значения в столбце **Значение**.
7. Нажмите на кнопку **Сохранить**.

Запись будет изменена.

Ограничения, действующие при редактировании записи:

- Значение ключевого поля записи недоступно для редактирования. Вы можете изменить его с помощью операций экспорта и импорта записи.
- Редактирование названий полей в столбце **Поле** недоступно.
- Значения в столбце **Значение** должны соответствовать следующим требованиям:
  - больше или равно 0 для полей типов **Временная метка** и **Список временных меток**;
  - соответствует формату IPv4 или IPv6 для полей типов **IP-адрес** и **Список IP-адресов**;
  - равно **true** или **false** для поля типа **Логический тип**.

Удаление записи из контекстной таблицы

Чтобы удалить записи из контекстной таблицы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, из контекстной таблицы которого вы хотите удалить запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.

5. Установите флажки для записей, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   > Должен быть установлен хотя бы один флажок.

6. Нажмите на кнопку **Удалить**.

7. Нажмите на кнопку **OK**.

Записи будут удалены.

Импорт данных в контекстную таблицу

Чтобы импортировать данные в контекстную таблицу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите импортировать данные, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. Установите флажок рядом с нужной контекстной таблицей и нажмите на кнопку **Импортировать**.

   Откроется окно импорта данных в контекстную таблицу.

5. Нажмите **Добавить** и выберите файл, который требуется импортировать.

6. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**
   - **tsv**
   - **internal**

7. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в контекстную таблицу. Записи, внесенные в контекстную таблицу ранее, сохраняются.

При импорте KUMA проверяет уникальность ключа каждой записи. Если запись уже существует, то в ее поля записываются новые значения, полученные слиянием прежних значений со значениями полей импортируемой записи.

Если записи в контекстной таблице не существовало, то создается новая запись.

> При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в виджетах, при наличии недопустимых символов в данных виджеты будут отображаться некорректно.

Экспорт данных из контекстной таблицы

Чтобы экспортировать данные из контекстной таблицы:

1. В главном окне приложения перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. Выберите коррелятор, контекстную таблицу которого вы хотите экспортировать, и в панели инструментов или в меню (⋮) нажмите **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
3. Установите флажок рядом с контекстной таблицей, которую нужно экспортировать.

   Вы не можете экспортировать несколько контекстных таблиц одновременно. Каждую таблицу нужно экспортировать отдельно.
4. Нажмите на кнопку **Экспортировать** и в раскрывающемся списке **Формат** выберите нужный формат:
   - **internal**.

     Контекстная таблица будет экспортирована в формате JSON.
   - **csv**.
   - **tsv**.
5. Нажмите на кнопку **Экспортировать**.

Контекстная таблица будет загружена на ваше устройство в выбранном формате. Название экспортированного файла формируется по шаблону: <название контекстной таблицы>_<дата экспорта (ГГГГ-ММ-ДД)>_<время экспорта (ЧЧ-ММ-СС)>. При экспорте данные в файле сортируются по полю **Ключ**.

При экспорте в формате JSON (**internal**):

- Порядок полей в файле не определен.
- Поля с типом массив экспортируются в файл в виде массива значений, например: `["val1","val2","val3","val4"]`.
- Формат даты и времени в поле с типом **Временная метка** зависит от выбранного языка интерфейса приложения:
  - Русский: ДД.ММ.ГГГГ ЧЧ:ММ:СС, например, `18.02.2025 16:09:58`
  - English: ГГГГ-ММ-ДД ЧЧ:ММ:СС, например, `2025.02.18 16:09:58`

При экспорте в форматах CSV и TSV:

- В первой строке файла указаны названия полей, строки ниже содержат данные.
- Для формата CSV в качестве разделителя полей используется запятая, а для формата TSV – знак табуляции.

Вы также можете экспортировать данные из контекстной таблицы в окне изменения параметров контекстной таблицы.

Построение иерархии экземпляров OSMP

Вы можете организовать экземпляры Open Single Management Platform (OSMP) в двухуровневую иерархию с родительским экземпляром наверху. Это позволит передавать параметры родительского экземпляра дочерним экземплярам, сохраняя при этом параметры дочерних экземпляров.

Например, Пользователь A и Пользователь B развернули OSMP. Оба пользователя имеют независимый экземпляр OSMP и работают в собственном экземпляре Консоли OSMP.

Чтобы обеспечить обмен данными между экземплярами, Пользователю A и Пользователю B нужно организовать свои экземпляры в иерархию. Для этого Пользователь A, пользователь будущего дочернего экземпляра, отправляет запрос на подключение к будущему родительскому экземпляру, где Пользователь B, пользователь будущего родительского экземпляра, подтверждает запрос.

При необходимости вы можете отключить дочерний экземпляр.

После построения иерархии объекты экземпляров управляются в иерархии следующим образом:

- **Серверы администрирования**

  В иерархии экземпляров вам нужно вручную назначить подчиненный Сервер администрирования.

- **Тенанты**

  Иерархия тенантов дочернего экземпляра встроена в иерархию тенантов родительского экземпляра. Параметры тенанта и параметры тенанта интеграции дочернего экземпляра можно изменить как в дочернем, так и в родительском экземплярах. Параметры тенанта и параметры тенанта интеграции родительского экземпляра можно изменить только из родительского экземпляра.

  В родительском экземпляре вы можете просматривать иерархию тенантов дочернего экземпляра, создавать, изменять и удалять тенанты дочернего экземпляра, но удалить дочерний экземпляр тенанта Root невозможно.

- **Активы (устройства) и категории активов**

  Параметры родительского и дочернего экземпляров не зависят друг от друга. Если вы вносите изменения в родительский экземпляр, изменения не применяются к дочернему, и наоборот.

  В дочернем экземпляре активы родительского экземпляра не отображаются. В дочернем экземпляре доступны просмотр категорий активов родительского экземпляра, привязка активов дочернего экземпляра и выполнение действий по реагированию для активов дочернего экземпляра. Например, для родительского экземпляра и для дочернего экземпляра существует категория активов NNN. Если вы запускаете действие по реагированию для категории NNN из дочернего экземпляра, действие по реагированию выполняется только с активами дочернего экземпляра. Вы не можете изменять категории родительских экземпляров, назначать эти категории устройствам дочерних экземпляров или создавать подкатегории унаследованных категорий.

  В родительском экземпляре отображаются категории активов дочернего экземпляра. Если вы выберете категорию актива, отобразятся активы дочернего экземпляра. Вы можете выполнять действия по реагированию для активов категорий дочерних экземпляров. Если нет подключения к дочернему экземпляру, пользователь родительского экземпляра может инициировать действие по реагированию, которое будет выполнено на устройствах дочернего экземпляра после восстановления подключения. Если вы удаляете категорию из родительского экземпляра, то в дочернем экземпляре эта категория становится локальной и перемещается в категорию Категоризованные активы на тенанте Root дочернего экземпляра. Вы не можете удалить категорию активов, если она используется ресурсами KUMA. Категории активов дочернего экземпляра не могут использоваться ресурсами KUMA родительского экземпляра.

- **Пользователи и роли пользователей**

Все пользователи управляются из родительского экземпляра. Пользователи и роли реплицируются из родительского экземпляра в дочерний (кроме учетной записи admin). В дочернем экземпляре существующие пользователи удаляются, а роли пользователей остаются без репликации в родительский экземпляр.

Учетная запись admin уникальна для каждого экземпляра OSMP и не реплицируется между экземплярами. Поэтому под учетной записью admin родительского экземпляра не поддерживаются следующие действия:

- Работа с событиями дочернего экземпляра в разделе **Поиск угроз** родительского экземпляра;
- Просмотр информации о ресурсах дочерних экземпляров из родительского экземпляра;
- Просмотр и управление сервисами дочерних экземпляров из родительского экземпляра.

- **Файлы**

  Файлы, загруженные и полученные в результате действий по реагированию, выполненных на дочернем экземпляре, отображаются в таблице файлов в родительском экземпляре в поле **Тенант** со следующим значком: (). Открывая сведения о файле дочернего экземпляра в родительском экземпляре, вы перенаправляетесь на дочерний экземпляр для дальнейших операций с файлом.

- **Объекты KUMA**

  - **События**

    События дочернего экземпляра хранятся в дочернем экземпляре, события родительского экземпляра хранятся в родительском экземпляре. В родительском экземпляре вы можете выполнить поиск событий дочерних экземпляров.

  - **Правила корреляции и IOA-правила**

    После построения иерархии IOA-правила преобразуются в правила корреляции KUMA.

    Существуют следующие режимы работы с правилами корреляции в иерархии:

    - **Локальный**. Если правило корреляции создано в дочернем экземпляре, оно управляется и в дочернем экземпляре. Если правило корреляции унаследовано от родительского экземпляра, то на дочернем экземпляре вы можете только добавлять исключения в правило корреляции и не можете изменять правило.

      Правила корреляции и их исключения применяются только к устройствам, подключенным к Серверу администрирования дочернего экземпляра.

    - **Глобальный**. Правила корреляции создаются в родительском экземпляре. Правила и их исключения применяются к устройствам дочернего экземпляра, которые вы указали при настройке параметров правил.

  - **Исключения правил корреляции**

    Временные исключения, добавленные в правила корреляции в родительском экземпляре, не наследуются. В дочернем экземпляре вы можете добавить временное исключение к унаследованным правилам корреляции. Фильтры наследуются с правилами корреляции.

- **Алерты и инциденты**

  Алерты и инциденты дочернего экземпляра реплицируются в родительский экземпляр и отображаются как в дочернем, так и в родительском экземплярах. Алерты и инциденты родительского экземпляра отображаются только в родительском экземпляре. В родительском экземпляре вы не можете изменять, привязывать и объединять алерты или инциденты дочернего экземпляра.

  При удалении алертов или инцидентов в дочернем экземпляре они также удаляются из родительского экземпляра.

Параметры алертов и инцидентов, а также срок хранения не наследуются. Если срок хранения истекает и алерт или инцидент удаляются в дочернем экземпляре, соответствующее событие отправляется в родительский инцидент, а затем алерт или инцидент также удаляется в родительском экземпляре.

- **Типы инцидентов**, **рабочие процессы** и **SLA**

  Чтобы избежать несогласованности данных, типы инцидентов, рабочие процессы и SLA копируются в дочерний экземпляр как единый пакет.

  - **SLA.**

    На дочернем экземпляре создать SLA невозможно. При попытке просмотреть дочерний SLA родительского экземпляра вы будете перенаправлены на дочерний экземпляр.

  - **Рабочий процесс**

    В дочернем экземпляре вы можете создавать рабочие процессы, а также просматривать и применять рабочие процессы, унаследованные от родительского экземпляра. При попытке просмотреть рабочий процесс дочернего экземпляра из родительского экземпляра вы будете перенаправлены на дочерний экземпляр. В родительском экземпляре вы можете удалять рабочие процессы родительского экземпляра: если рабочий процесс не имеет связанных объектов в родительском экземпляре, рабочий процесс больше не отображается и через 90 дней полностью удаляется. Вы не можете удалить рабочий процесс, если у него есть связанные объекты.

  - **Типы инцидентов**

    Типы инцидентов наследуются от родительского экземпляра, в котором у них статус выключен. Если тип инцидента по умолчанию наследуется, то в дочернем экземпляре этот тип инцидента не используется по умолчанию.

    В дочернем экземпляре вы можете создавать новые типы инцидентов, а также просматривать и применить унаследованные типы инцидентов. Вы не можете изменять унаследованные типы инцидентов. Также вы можете использовать атрибут по умолчанию как для унаследованных типов инцидентов, так и для тех, которые созданы локально в дочернем экземпляре.

- **Правила агрегации**

  Правила агрегации, созданные вручную, наследуются от родительского экземпляра. Предустановленные правила агрегации не наследуются.

  В родительском экземпляре вы можете просмотреть все правила агрегации дочернего экземпляра. Возможность изменять правила определяется вашей EDR-ролью.

  В дочернем экземпляре унаследованные правила агрегации отображаются в верхней части таблицы правил в том порядке, в котором они отображались в родительском экземпляре. По умолчанию правила при наследовании выключены. Вы можете просматривать, включать и выключать унаследованные правила агрегации.

  Включенные правила агрегации будут применяться в соответствии с их приоритетом: чем выше правило в таблице, тем выше его приоритет.

- **Правила сегментации**

  Правила сегментации, созданные вручную, наследуются от родительского экземпляра. Предустановленные правила сегментации не наследуются.

  В родительском экземпляре вы можете просмотреть все правила сегментации дочернего экземпляра. Возможность изменять правила определяется вашей EDR-ролью.

  В дочернем экземпляре унаследованные правила сегментации отображаются в верхней части таблицы правил в том порядке, в котором они отображались в родительском экземпляре. По умолчанию правила при наследовании выключены. Вы можете просматривать, включать и выключать унаследованные правила сегментации.

Включенные правила сегментации будут применяться в соответствии с их приоритетом: чем выше правило в таблице, тем выше его приоритет.

- **Правила запрета**

  Правила запрета наследуются от родительского экземпляра.

  В родительском экземпляре вы можете просматривать и изменять правила запрета дочернего экземпляра, а также применять правила дочернего экземпляра к активам дочернего экземпляра. Вы не можете применить правила запрета дочернего экземпляра к активам родительского экземпляра.

  В дочернем экземпляре можно просматривать правила запрета, унаследованные от родительского экземпляра. Эти правила невозможно изменять, также невозможно добавлять или удалять активы дочернего экземпляра в правилах запрета, унаследованных от родительского экземпляра.

- **YARA- и IOC-правила**

  Списки YARA-правил и IOC-правил наследуются от родительского экземпляра.

  В родительском экземпляре вы можете просматривать и изменять правила дочернего экземпляра, а также применять правила дочернего экземпляра к активам дочернего экземпляра. Вы не можете применять правила дочернего экземпляра к активам родительского экземпляра.

  В дочернем экземпляре вы можете просматривать YARA-правила и IOC-правила, унаследованные от родительского экземпляра, но не можете изменять эти правила. Для выполнения действий по реагированию вы можете использовать как правила дочернего экземпляра, так и правила, унаследованные от родительского экземпляра.

- **Правила Sandbox**

  Правила Sandbox наследуются от родительского экземпляра.

  В родительском экземпляре вы можете просматривать и изменять правила дочернего экземпляра Sandbox, а также применять правила дочернего экземпляра к активам дочернего экземпляра.

  В дочернем экземпляре вы можете просматривать правила Sandbox, унаследованные от родительского экземпляра, но не можете изменять эти правила.

- **Плейбуки**

  В родительском экземпляре вы можете создавать плейбуки в дочернем экземпляре и вручную запускать плейбуки для алертов и инцидентов дочернего экземпляра.

- **Лицензирование**

  Управление лицензиями и настройка параметров лицензирования выполняются экземплярами независимо друг от друга и не наследуются в иерархии экземпляров.

  Лицензионный ключ добавляется для каждого экземпляра отдельно. Вы можете добавить один и тот же лицензионный ключ для всех экземпляров.

- **Политики и задачи**

  Политики и задачи наследуются от родительского экземпляра.

- Параметры KSN/KPSN, учетные данные и шаблоны уведомлений не наследуются.

Подключение дочернего экземпляра к родительскому экземпляру

Пользователь будущего дочернего экземпляра отправляет запрос на подключение, а пользователь будущего родительского экземпляра подтверждает этот запрос.

У обоих пользователей должна быть EDR-роль Главного администратора в своих экземплярах.
Если вы отправляете запрос на подключение к экземпляру, который служит дочерним экземпляром в другой иерархии, запрос будет отменен.
Максимальное количество дочерних экземпляров, которое может иметь родительский экземпляр, равно 150.

Отправка запроса на подключение от дочернего экземпляра

Чтобы отправить запрос на подключение:

1. В главном меню будущего дочернего экземпляра перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. В панели инструментов нажмите на кнопку **Запросить соединение**.

3. В открывшейся правой панели выполните следующее:

   - В поле **API URL родительского экземпляра** укажите адрес публичного API родительского экземпляра, например `https://api.xdr-hier-1.kuma.example.com`.

   - В поле **Отпечаток сертификата родительского экземпляра** укажите хеш файла сертификата родительского экземпляра.

     Нажмите на кнопку **Получить отпечаток**, чтобы вставить хеш сертификата родительского экземпляра в файл **Отпечаток сертификата родительского экземпляра**. Если у родительского экземпляра есть цепочка сертификатов, Kaspersky EDR Expert использует промежуточный сертификат. Не рекомендуется использовать конечный сертификат, потому что его ротация происходит чаще, чем промежуточного сертификата. После ротации указанного сертификата необходимо восстановить иерархию экземпляров.

   - В поле **API-токен** укажите публичный API-токен для внешних интеграций.

     Токен API должен быть предварительно сгенерирован на родительском экземпляре.
     При настройке параметров токена методы API GET:/api/hierman/v1/* и POST:/api/hierman/v1/* являются обязательными для построения иерархии экземпляров.

- При необходимости настройте следующие параметры:
  - В поле **API URL дочернего экземпляра** укажите адрес публичного API дочернего экземпляра, например *https://api.xdr-hier-2.kuma.example.com*.
  - В разделе **Выбор тенантов для совместного использования ресурсов SIEM** установите флажки рядом с тенантами, к SIEM ресурсам которых вы хотите иметь доступ в родительском экземпляре.

4. Нажмите на кнопку **Запрос**.

   Панель будет закрыта.

5. В диалоговом окне нажмите на кнопку **Запрос**.

   Диалоговое окно подтверждения закроется и отобразится сообщение о состоянии: **Ваш запрос на подключение ожидает подтверждения**.

После того как пользователь родительского экземпляра подтвердит или отклонит запрос, вы получите уведомление по электронной почте, а также изменится отображаемое сообщение о состоянии запроса.

Когда пользователь родительского экземпляра подтвердит запрос, идентификатор родительского экземпляра и имя тенанта родительского экземпляра отобразятся в дочернем экземпляре.

Подтверждение запроса на подключение от родительского экземпляра

После того как пользователь дочернего экземпляра отправил запрос на подключение, вы получите соответствующее уведомление по электронной почте.

Чтобы подтвердить запрос на подключение:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Вверху страницы перейдите по ссылке **Просмотреть запросы**, которая отображается в сообщении об ожидающих запросах на подключение.
3. В открывшейся панели **Запросы на подключение** нажмите на кнопку **Подтвердить** для запроса, который вы хотите подтвердить.
4. В открывшейся панели **Подтвердить запрос на подключение** выполните следующие действия:
   - В поле **Название корневого тенанта** укажите новое название для подключаемого тенанта дочернего экземпляра.
   - В разделе **Название корневого тенанта** из иерархии тенантов родительского экземпляра выберите тенант, который будет назначен в качестве родительского для тенанта дочернего экземпляра.
   - Нажмите на кнопку **Подтвердить**.

     Панель будет закрыта.

   Дочерний экземпляр добавлен в иерархию тенантов родительского экземпляра. Соответствующее сообщение отобразится на экране.

Перезапуск активных служб на дочернем экземпляре

После того как подключение между дочерним и родительским экземплярами установлено, перезапустите активные сервисы на дочернем экземпляре. После этого активные сервисы дочернего экземпляра будут отображаться на родительском экземпляре.

Результаты

Теперь вы можете управлять деревом тенантов дочернего экземпляра следующим образом:

- Просматривать дерево тенантов дочернего экземпляра.
- Создавать тенанты в дочернем экземпляре.
- Изменять тенанты в дочернем экземпляре.
- Удалять тенанты из дочернего экземпляра, кроме тенанта Root.
- Отключить дочерний экземпляр.

Пользователь дочернего экземпляра может просматривать, изменять и удалять тенанты только дочернего экземпляра.

Назначение подчиненного Сервера администрирования в иерархии экземпляров OSMP

После построения иерархии экземпляров OSMP необходимо вручную установить отношение "главный/подчиненный", вручную назначив подчиненный Сервер администрирования.

Чтобы назначить Сервер администрирования, доступный для подключения через Консоль OSMP, в качестве подчиненного Сервера:

1. На будущем главном Сервере администрирования убедитесь, что порт 13000 доступен для приема подключений от подчиненных Серверов администрирования.
2. В главном окне приложения нажмите на имя Сервера администрирования, чтобы открыть окно свойств, а затем перейдите на вкладку **Серверы администрирования**.
3. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.
4. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. Укажите параметры подключения для будущего подчиненного Сервера администрирования:

   - **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

     Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

     Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

   - **Адрес подчиненного Сервера администрирования (необязательно)**

     Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

     Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

   - **SSL-порт Сервера администрирования**

     Укажите номер SSL-порта главного Сервера администрирования. По умолчанию установлен порт 13000.

     Для корневого Сервера администрирования используется порт 13000, и изменить его нельзя.

   - **API-порт Сервера администрирования**

     Номер порта, который Web Console будет использовать для приема подключений от подчиненного Сервера администрирования по OpenAPI. По умолчанию установлен порт 13299.

     При построении иерархии Web Console подключается к будущему подчиненному Серверу, запрашивает учетные данные, получает открытый сертификат и выполняет первоначальную настройку.

     После построения иерархии Сервера администрирования порт 13299 больше не будет использоваться. Серверы администрирования будут взаимодействовать через порт 13000.

6. Укажите сертификат будущего подчиненного Сервера.

   Если выбран параметр **Адрес подчиненного Сервера администрирования (необязательно)**, вам нужно либо нажать на кнопку **Получить с подчиненного Сервера администрирования**, чтобы получить сертификат, либо нажать на кнопку **Выбрать файл сертификата**, чтобы добавить сертификат вручную.

7. Укажите адрес будущего главного Сервера.

8. Если подключение к будущему главному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

9. Укажите учетные данные пользователя, имеющего права доступа к будущему подчиненному Серверу администрирования.

10. Если двухфакторная аутентификация включена и настроена, укажите секретный ключ, сгенерированный приложением для аутентификации.

11. Сохраните параметры.

12. Переключитесь к будущему подчиненному Серверу администрирования и откройте его свойства.

13. На вкладке **Общие** перейдите в раздел **Иерархия Серверов администрирования** и выполните следующие действия:

    - Выберите параметр **Этот Сервер администрирования является подчиненным в иерархии**.
    - В поле **Адрес главного Сервера администрирования** укажите сетевое имя будущего главного Сервера администрирования.
    - Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку Обзор.
    - Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
    - Если подключение к будущему главному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

14. Сохраните параметры.

Иерархия "главный/подчиненный" Серверов администрирования построена. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Отключение дочернего экземпляра от родительского экземпляра

После отключения дочернего экземпляра от его родительского экземпляра вы не можете подключить дочерний экземпляр к другой иерархии.

Отключение от родительского экземпляра

Чтобы отключить дочерний экземпляр:

1. В главном меню родительского экземпляра перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Установите флажок рядом с дочерним экземпляром тенанта Root, который нужно отключить.

3. В панели инструментов нажмите на кнопку **Отключить** и в открывшемся окне подтверждения нажмите **Отключить**.

Дочерний экземпляр будет отключен от родительского и на экране отобразится соответствующее сообщение. Пользователь дочернего экземпляра получит уведомление по электронной почте.

Если в момент разрыва соединения дочерний экземпляр выключен, соединение разрывается принудительно. Чтобы завершить отключение дочернего экземпляра от родительского, включите дочерний экземпляр и следуйте инструкциям ниже.

При отключении экземпляров Kaspersky EDR Expert создает событие аудита `Отключение SCN от PCN`. В обоих случаях, если дочерний экземпляр включен или выключен в момент отключения, событие аудита будет одинаковым.

В целях диагностики, если дочерний экземпляр в момент отсоединения выключен, Kaspersky EDR Expert добавляет ошибку в файлы журнала компонента hierman, например ошибку "disconnect on secondary failed". Используйте значение поля `trace_id` в событии аудита, чтобы найти ошибки в файлах журнала.

Отключение от дочернего экземпляра

Чтобы отключить дочерний экземпляр:

1. В главном меню дочернего экземпляра перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Установите флажок рядом с тенантом Root, который нужно отключить.

3. В панели инструментов нажмите на кнопку **Отключить** и в открывшемся окне подтверждения нажмите **Отключить**.

Дочерний экземпляр будет отключен от родительского и на экране отобразится соответствующее сообщение. Пользователь родительского экземпляра получит уведомление по электронной почте.

Результаты отключения экземпляров

В результате отключения дочернего экземпляра иерархия OSMP будет нарушена.

В родительском экземпляре:

- Ресурсы и параметры отключенного экземпляра удаляются.

- Данные дочернего экземпляра, реплицированные в родительский экземпляр, теперь удаляются из родительского экземпляра.

В дочернем экземпляре:

- Информация о родительском экземпляре удаляется, и родительский экземпляр не отображается в иерархии тенантов дочернего экземпляра.

- Управление иерархией тенантов дочернего экземпляра возвращается к дочернему экземпляру.

- Identity and Access Manager остается доступным только для чтения.

  Пользователи дочернего экземпляра могут войти в экземпляр, но не могут выполнять другие действия (создавать пользователей, назначать права, изменять пароль).

Пользователи, созданные в дочернем экземпляре до того, как экземпляр был подключен к иерархии, удаляются из дочернего экземпляра.

- Объекты, унаследованные от родительского экземпляра, сразу удаляются из дочернего экземпляра, если у объектов нет связанных объектов в родительском экземпляре. Иначе объект больше не отображается в дочернем экземпляре, но остается доступный для чтения в течение 90 дней. По прошествии этого срока объекты удаляются.

- Активы, унаследованные от родительской категории, теперь управляются в дочернем экземпляре.

- Службы, управляемые родительским экземпляром, удаляются.

Распределение правил корреляции в иерархии

В OSMP поддерживается централизованное управление и распространение правил корреляции между экземплярами OSMP, объединенными в иерархию.

Вы можете создавать правила корреляции на родительском экземпляре OSMP и автоматически распространять их на дочерние экземпляры. На дочерних экземплярах OSMP унаследованные правила корреляции используются без возможности изменения. Для внесения изменений необходимо создать локальную копию унаследованного правила (дублировать правило корреляции). После этого изменения выполняются только в локальной копии. Путь к ресурсу на родительском и дочерних экземплярах OSMP будет отличаться, поскольку у папок разные имена, при этом сами ресурсы и изменения в них будут синхронизированы.

Централизованное управление обеспечивает единое использование правил корреляции в распределенных инфраструктурах с несколькими экземплярами OSMP, снижает затраты на сопровождение правил и поддерживает единообразное обнаружение угроз.

Основные термины

Глобальное правило — правило корреляции, созданное на родительском экземпляре OSMP и распространяемое на дочерние экземпляры.

Локальное правило – правило, созданное на дочернем экземпляре OSMP.

Унаследованный коррелятор – сервис корреляции на дочернем экземпляре OSMP, использующий конфигурацию коррелятора, созданную на родительском экземпляре.

Унаследованный ресурс – ресурс, полученный из родительского экземпляра OSMP по иерархии.

Предварительные условия

Для работы механизма наследования правил должны быть выполнены следующие условия:

1. Настроена иерархия экземпляров OSMP.

   Экземпляры OSMP должны быть объединены в иерархию: родительский экземпляр и один или несколько дочерних экземпляров.

2. Дочерний экземпляр OSMP подключен к родительскому экземпляру OSMP.

Возможности функции

На родительском экземпляре OSMP доступны следующие действия:

- Создание глобальных правил корреляции и распространение правил на дочерние экземпляры OSMP.
- Просмотр ресурсов и сервисов, созданных на дочерних экземплярах OSMP.

В разделе **Активные сервисы** доступны следующие операции:

- Добавление сервиса.
- Обновление параметров сервиса.
- Перезапуск сервиса.
- Удаление сервиса дочернего экземпляра.
- Просмотр событий сервиса.
- Просмотр активных листов.
- Просмотр контекстных таблиц.
- Просмотр разделов.
- Скачивание логов и дампа.
- Копирование идентификатора сервиса.
- Копирование идентификатора кластера.
- Сброс сертификата.

На дочернем экземпляре OSMP доступны следующие действия:

- Использование унаследованных правил без возможности редактирования.
- Создание локальной копии глобального правила.

В разделе **Активные сервисы** для унаследованных сервисов доступны следующие операции:

- Просмотр журналов сервиса.
- Обновление параметров сервиса.
- Просмотр конфигурации сервиса.

Ограничения

Для унаследованных правил корреляции на дочерних экземплярах OSMP недоступно изменение правил, удаление, изменение привязки к сервисам, изменение параметров коррелятора.

Для изменения унаследованного правила корреляции необходимо создать его дубликат на дочернем экземпляре OSMP.

Дубликат становится локальным ресурсом, доступным для внесения изменений.

Жизненный цикл правил

Обновление родительского правила

После изменения глобального правила изменения не распространяются автоматически. Если вы хотите применить изменения, необходимо выполнить перезапуск сервиса коррелятора или

обновление параметров сервиса.

После этого изменения будут применены на дочерних экземплярах OSMP.

Удаление правила на родительском экземпляре

Если глобальное правило удалено на родительском экземпляре OSMP, на дочернем экземпляре OSMP унаследованное правило не удаляется автоматически. Унаследованное правило становится локальным и дочерний экземпляр OSMP получает полные права на ресурс.

Дублирование правила

Если глобальное правило продублировано на дочернем экземпляре OSMP, создается локальная копия правила и дочерний экземпляр OSMP получает полные права (чтение, запись, удаление).

Экспорт и импорт

Унаследованное правило можно экспортировать и импортировать в другой экземпляр OSMP.

После импорта такое правило становится локальным ресурсом, доступным для внесения изменений.

Временное нарушение связи

Если соединение между экземплярами OSMP временно отсутствует, пакеты до 64 МБ передаются сразу, более крупные пакеты отклоняются с ошибкой.

После восстановления соединения дочерние экземпляры получают недостающие изменения.

Разрыв иерархии

Если дочерний экземпляр отключен от иерархии, унаследованные сервисы становятся локальными, унаследования правила становятся локальными и доступны для изменения и удаления.

Сценарии использования

Доступны следующие возможности:

- Распространение глобальной конфигурации коррелятора с глобальным правилом корреляции.
- Распространение глобального правила корреляции для локального использования.
- Дублирование унаследованного правила корреляции на дочернем экземпляре OSMP.
- Просмотр правил корреляции, созданных на дочерних экземплярах OSMP.

Распространение глобальной конфигурации коррелятора вместе с глобальными правилами корреляции

Чтобы распространить глобальные правила на дочерние экземпляры OSMP в рамках наследуемого коррелятора:

1. На родительском экземпляре OSMP выполните следующие действия:

   a. Создайте глобальное правило корреляции:

      1. Перейдите в раздел **Ресурсы и сервисы** → **Правила корреляции**.
      2. Создайте правило корреляции.
      3. В параметрах правила корреляции переведите переключатель **Включить наследование на вторичных узлах** в активное положение.
      4. В раскрывающемся списке укажите тенант или несколько тенантов дочерних экземпляров OSMP, в которые необходимо передать правило.
      5. Сохраните правило корреляции.

      Созданное правило корреляции необходимо привязать к сервису коррелятора.

   b. Создайте сервис коррелятора, который будет наследоваться на дочерних экземплярах OSMP, и привяжите глобальное правило корреляции:

      1. Перейдите в раздел **Ресурсы и сервисы** → **Корреляторы**.
      2. Создайте коррелятор и в мастере установки на шаге **Общие** переведите переключатель **Включить наследование на вторичных узлах** в активное положение.

3. В раскрывающемся списке укажите тенант или несколько тенантов дочерних экземпляров OSMP, в которые необходимо передать конфигурацию коррелятора.

4. На шаге мастера установки **Корреляция** привяжите глобальное правило корреляции.

5. Сохраните параметры сервиса коррелятора.

После сохранения параметров конфигурация сервиса коррелятора и глобальное правило корреляции сохраняются на родительском экземпляре OSMP и передаются на дочерние экземпляры OSMP. Дальнейшая настройка конфигурации сервиса коррелятора и установка сервиса коррелятора выполняется на дочерних экземплярах OSMP.

2. На дочернем экземпляре OSMP выполните следующие действия:

   a. Перейдите в раздел **Ресурсы и сервисы** → **Корреляторы** и в таблице сервисов откройте унаследованный сервис коррелятора.

      1. В мастере установки коррелятора на шаге **Маршрутизация** укажите точку назначения:

      - Хранилище, в котором будут сохраняться события и алерты.

      - Коррелятор на родительском экземпляре OSMP для дальнейшей обработки событий.

      1. На шаге **Проверка параметров** выберите **Сохранить и создать сервис**.

      2. Скопируйте команду установки в блоке **Рекомендуемая команда установки коррелятора** и установите сервис коррелятора на хосте дочернего экземпляра OSMP.

В результате на дочернем экземпляре OSMP:

- Создается копия правила корреляции.

- Создаются связанные зависимые ресурсы.

- Создается унаследованная конфигурация коррелятора. Ресурсы, используемые внутри коррелятора, также наследуются, даже если они не наследуются отдельно, например, правила реагирования.

- Правило корреляции и конфигурация сервиса коррелятора доступны в режиме чтения с возможностью указывать точки назначения.

- Сервис отображается на родительском экземпляре OSMP в разделе **Активные сервисы** с признаком унаследованного сервиса.

- Изменения, внесенные на родительском экземпляре OSMP, автоматически наследуются вниз по иерархии.

Распространение глобальных правил корреляции для локального использования

Чтобы распространить глобальные правила на дочерние экземпляры OSMP с привязкой к локальному коррелятору:

1. На родительском экземпляре OSMP выполните следующие действия:

   a. Перейдите в раздел **Ресурсы и сервисы** → **Правила корреляции**.

   b. Создайте правило корреляции.

   c. В параметрах правила корреляции переведите переключатель **Включить наследование на вторичных узлах** в активное положение.

   d. В раскрывающемся списке укажите тенант или несколько тенантов дочерних экземпляров OSMP, в которые необходимо передать правило.

   e. Заполните остальные необходимые поля.

   f. Сохраните правило.

   Созданное глобальное правило корреляции будет передано на дочерние экземпляры OSMP. Унаследованное правило корреляции необходимо привязать к сервису коррелятора.

2. На дочернем экземпляре OSMP выполните следующие действия:

   a. Перейдите в раздел **Ресурсы и сервисы** → **Корреляторы**.

   b. Создайте сервис коррелятора или откройте параметры существующего сервиса.

   c. В мастере установки коррелятора на шаге **Корреляция** привяжите глобальное правило корреляции к локальному сервису коррелятора.

   d. Настройте остальные необходимые параметры.

e. На шаге **Проверка параметров** выполните одно из следующих действий:

- Если вы хотите создать коррелятор, нажмите **Сохранить и создать сервис**, а затем используйте сформированную команду для установки сервиса на хосте в дочернем экземпляре OSMP.
- Если вы хотите обновить параметры действующего коррелятора, нажмите **Сохранить и обновить параметры сервисов**.

В результате на дочернем экземпляре OSMP:

- Создается копия правила корреляции.
- Сервис коррелятора отображается в родительском экземпляре OSMP в разделе **Активные сервисы** и доступен для просмотра.
- Изменения, внесенные в правило корреляции на родительском экземпляре OSMP, автоматически наследуются вниз по иерархии.

Унаследованные правила корреляции доступны только в режиме чтения.

Если требуется изменить правило для локального использования, продублируйте правило корреляции и используйте локальную копию независимо от родительского экземпляра OSMP.

Дублировать унаследованные правила корреляции для локального использования

Предварительные условия:

- Настроена иерархия экземпляров OSMP.
- Дочерний экземпляр OSMP подключен к родительскому экземпляру.
- На родительском экземпляре OSMP создано правило корреляции.
- Настроено наследование глобального правила корреляции на дочерний экземпляр OSMP.

Чтобы дублировать унаследованные правила корреляции для локального использования:

1. На дочернем экземпляре OSMP перейдите в раздел **Ресурсы и сервисы** → **Правила корреляции**.
2. В таблице правил корреляции найдите унаследованное правило и установите рядом флажок.
3. На панели инструментов или в меню (⋮) нажмите **Дублировать**.
4. Укажите новое имя правила корреляции.
5. Сохраните копию правила корреляции.
6. Откройте созданную локальную копию правила корреляции.

7. Внесите необходимые изменения.

8. Сохраните правило корреляции.

В результате на дочернем экземпляре OSMP локальная копия правила корреляции становится независимой от родительского экземпляра OSMP и становится доступно редактирование параметров, удаление, экспорт, изменение зависимых ресурсов.

Ограничения:

После дублирования изменения родительского правила не применяются к локальной копии и не синхронизируются.

Просмотр ресурсов и сервисов, созданных в дочерних экземплярах OSMP

Предварительные условия:

- Настроена иерархия экземпляров OSMP.
- Дочерний экземпляр OSMP подключен к родительскому экземпляру OSMP.
- На дочернем экземпляре OSMP созданы ресурсы или сервисы.

Чтобы просмотреть ресурсы, созданные на дочерних экземплярах OSMP:

1. На родительском экземпляре OSMP перейдите в раздел **Ресурсы и сервисы** → **Правила корреляции**.
2. Откройте список ресурсов.
3. Просмотрите минимально доступную информацию:
   - Идентификатор.
   - Название.
   - ID тенанта.
   - Название тенанта.
   - Признак удаленного тенанта (тенанта дочернего экземпляра OSMP).
   - Тип правила.
   - Последнее обновление (дата).
   - Теги.
   - Техники MITRE.
   - Название пакета (если ресурс получен через серверы обновления "Лаборатории Касперского").

- Описание.
- Путь до ресурса.

  У папок на родительском и дочернем экземплярах будут разные названия, соответственно, пути будут различаться. При этом изменения будут синхронизироваться там, где это применимо.

Для просмотра полной информации откройте карточку правила корреляции.

Чтобы просмотреть сервисы корреляторов, созданные на дочерних экземплярах OSMP:

1. На родительском экземпляре OSMP перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.
2. В таблице сервисов откройте нужный сервис для просмотра.

В результате на родительском экземпляре OSMP:

- Отображаются ресурсы и сервисы дочерних экземпляров.
- Ресурсы и сервисы доступны только для просмотра.
- Доступен поиск и фильтрация.
- Полная информация правила корреляции загружается напрямую с дочернего экземпляра OSMP при открытии карточки ресурса.

На родительском экземпляре OSMP недоступны следующие действия с ресурсами дочерних экземпляров OSMP:

- Дублирование.
- Удаление.
- Просмотр списка зависимостей.
- Назначение тегов.
- Привязки к корреляторам.
- Назначения и просмотр списка исключений.
- Просмотр истории версий.
- Использование в корреляторах родительского экземпляра.

Поведение папок при распределении ресурсов в иерархии

Ресурсы привязываются к пути папки на момент распространения. Если не переименовывать и не перемещать папки вручную, маршрутизация не изменится. Изменения структуры папок не синхронизируются между экземплярами OSMP.

При распространении ресурсов по иерархии действуют следующие правила:

1. Передаются только те папки, которые содержат хотя бы один распространяемый ресурс.
2. Папки сопоставляются между экземплярами по их полному пути.
3. Идентификаторы папок не передаются: на целевом экземпляре папки создаются с новыми идентификаторами.
4. При импорте существующая структура папок не заменяется, а объединяется с полученной.
5. Операции над папками (создание, переименование, перемещение) напрямую не синхронизируются. Изменения становятся видимыми только через распространение ресурсов, находящихся в соответствующих папках.

Создание папки

Новая папка, созданная на дочернем экземпляре, не будет доступна для просмотра на родительском экземпляре OSMP до тех пор, пока в ней не будет создан хотя бы один распространяемый ресурс.

Переименование папки

Переименование папки не приводит к автоматическому обновлению структуры на других экземплярах OSMP.

После переименования следующее поведение является ожидаемым:

- Ресурсы, распространенные до изменения имени папки, остаются привязанными к старому пути.
- Ресурсы, распространенные после переименования, используют новый путь.

Пример

Исходное состояние:

- Родительский экземпляр: папка A, содержащая ресурс R1.
- Ресурс R1 наследуется на дочерний экземпляр.

Изменение:

- На дочернем экземпляре папка A переименована в B.
- В папке B создается новый ресурс R2 и распространяется на родительский экземпляр.

Результат:

- На родительском экземпляре R1 находится в папке A; R2 находится в папке B.
- На дочернем экземпляре: R1 и R2 находятся в папке B.

Каждый ресурс сохраняет привязку к тому пути папки, который существовал на момент его распространения. Поэтому для сохранения стабильной маршрутизации рекомендуется не переименовывать и не перемещать папки вручную.

Объединение экземпляров OSMP в иерархию

В этом разделе приведены инструкции по объединению экземпляров OSMP в иерархию.

1 Предварительные требования

Требуются два и более экземпляра OSMP – родительский экземпляр наверху и дочерний.

В этом разделе в качестве примеров используются следующие доменные имена:

- Для родительского экземпляра:
  - Для веб-интерфейса: `console.edrparent.organization.acme`
  - Для API: `api.edrparent.organization.acme`
- Для дочернего экземпляра:
  - Для веб-интерфейса: `console.edrchild1.organization.acme`
  - Для API: `api.edrchild1.organization.acme`
- Для всех экземпляров:
  - Требуется установить двустороннюю связь с портом 443 для IP-адреса каждого экземпляра.
  - Доменные имена для API дочерних узлов должны быть доступны для родительского экземпляра, а домен API родительской инсталляции должен быть доступен для всех дочерних узлов.

2 Подготовка родительского экземпляра

1. В главном меню будущего родительского экземпляра перейдите в раздел **Параметры** → **API-токены** и нажмите на кнопку **Добавить токен**.
2. В поле **Имя** укажите имя API-токена (например, `edrparenthierarchy`).

   Вы сможете отозвать этот токен позднее, после завершения подключения к дочернему узлу.

3. В поле **Срок действия** укажите срок действия токена. Эту дату требуется указывать с учетом минимального срока, необходимого для завершения построения иерархии (не менее одного дня).

4. В разделе **Методы API** установите флажки для следующих методов:

   - **GET:/api/hierman/v1/***
   - **POST:/api/hierman/v1/***

5. Нажмите **Сгенерировать**, затем нажмите **Копировать и закрыть**.

   API-токен будет создан и скопирован в буфер обмена. Сохраните его в надежном месте, поскольку в дальнейшем скопировать его будет невозможно.

6. Получите отпечаток сертификата, чтобы проверить подключение к экземпляру. Для этого откройте в браузере домен API родительского экземпляра (`api.edrparent.organization.acme`) и просмотрите сведения о сертификате.

   Убедитесь, что отпечаток поступил из доверенного источника. Проверьте его IP-адрес, чтобы убедиться, что домен не подменен.

3 Действия для каждого дочернего экземпляра

1. Перейдите к веб-интерфейсу будущего дочернего экземпляра (в этом примере `console.edrchild1.organization.acme`).

2. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

3. В панели инструментов нажмите на кнопку **Запросить соединение**.

4. В открывшейся правой панели выполните следующее:

   - В поле **API URL родительского экземпляра** укажите адрес API родительского экземпляра (в этом примере `api.edrparent.organization.acme`).
   - В поле **Отпечаток сертификата родительского экземпляра** укажите хеш файла сертификата родительского экземпляра.
   - В поле **API-токен** укажите API-токен, созданный ранее в родительском экземпляре.

5. Нажмите на кнопку **Запрос**.

   Если все поля заполнены правильно, будет отображено сообщение "*Ваш запрос отправлен*".

6. Перейдите к **родительскому** экземпляру (в этом примере `console.edrparent.organization.acme`).

7. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Будет отображено сообщение "*Ожидается запрос на подключение*". Если сообщение не отобразится, обновите страницу.

8. Нажмите **Просмотреть запрос**.

   Откроется окно с подробностями о дочернем экземпляре.

9. Внимательно проверьте заполненные поля и адрес. В особенности уделите внимание полю **Отпечаток сертификата** – его значение требуется проверять, используя доверенный источник сертификата дочернего экземпляра. Проверьте IP-адрес, чтобы убедиться, что домен (`api.edrchild1.organization.acme` в этом примере) не подменен.

10. Если все поля заполнены должным образом, нажмите на кнопку **Подтвердить**.

11. В открывшейся панели **Подтвердить запрос на подключение** выполните следующие действия:

    - В поле **Название корневого тенанта** укажите новое название для подключаемого тенанта дочернего экземпляра. Корневой тенант дочернего экземпляра будет зарегистрирован в родительском экземпляре с этим именем.

    - В разделе **Название корневого тенанта** из иерархии тенантов родительского экземпляра выберите тенант, который будет назначен в качестве родительского для тенанта дочернего экземпляра.

    - Нажмите на кнопку **Подтвердить**.

      Панель будет закрыта. Дочерний экземпляр добавлен в иерархию тенантов родительского экземпляра. На экране будет отображено сообщение "*Корневой тенант подключен к экземпляру*".

12. Обновите страницу – в дереве тенантов появится новый узел с иерархией дочерних экземпляров.

Восстановление иерархии экземпляров после ротации сертификатов

При построении иерархии экземпляров OSMP вы указываете сертификат родительского экземпляра в поле **Отпечаток сертификата родительского экземпляра**. После ротации указанного сертификата иерархия нарушается. Например, это может произойти по следующим причинам:

- Вы обновили Kaspersky EDR Expert с предыдущей версии или обновили ее до той же основной версии.

- Сертификат автоматически заменяется, когда истекает его срок действия.

- Вы заменили сертификат вручную.

Если иерархия нарушена, OSMP добавляет следующую ошибку в файлы журнала компонента hierman: "no certificate in chain matches expected thumbprint".

Чтобы восстановить иерархию экземпляров после ротации сертификатов:

1. На устройстве администратора родительского экземпляра OSMP выполните следующую команду:

   ```
   ./kdt invoke hierman --action hiermanRepairTrust
   ```

2. Выполните ту же команду на устройствах администратора дочерних экземпляров OSMP, включенных в иерархию.

Иерархия восстановлена.

Интерфейс Консоли OSMP

Управление Kaspersky EDR Expert осуществляется через интерфейс Консоли OSMP.

Окно Консоли OSMP содержит следующие элементы:

- главное меню в левой части окна;
- верхняя панель в верхней части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Нажмите на имя Сервера администрирования, чтобы открыть свойства Сервера администрирования.
- **Навигация консоли**. Отображает карту главного меню. Раздел **Навигация консоли** установлен как домашняя страница по умолчанию. Вы можете изменить эти параметры.
- **Мониторинг**. Предоставляет обзор вашей инфраструктуры, статусов защиты и статистики, включая поиск угроз, алерты и инциденты и плейбуки.
- **Управление активами**. Инструменты для управления активами и оборудованием, а также политики приложений "Лаборатории Касперского".
- **Задачи**. Содержит инструменты для создания и запуска задач.
- **Пользователи и роли**. Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Хранилища**. Предоставляет вам доступ к хранилищам приложений.
- **Управление программным обеспечением**. Позволяет управлять приложениями "Лаборатории Касперского" и приложениями сторонних производителей, а также инсталляционными пакетами и патчами.
- **Операции**. Позволяет выполнять различные операции, включая лицензирование приложений, просмотр и управление зашифрованными дисками и событиями шифрования.
- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. В этом разделе также содержится информация о мастере развертывания защиты.

- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".

- **Параметры**. Содержит параметры интеграции Kaspersky EDR Expert с другими приложениями "Лаборатории Касперского" и позволяет вам создать API-токены. Он также содержит параметры, связанные с отображением элементов интерфейса в зависимости от используемых функций и с языком интерфейса.

При необходимости вы можете свернуть главное меню до значков, нажав на значок стрелки (‹‹) внизу экрана.

Верхняя панель

Верхняя панель всегда отображается во всех разделах консоли и не может быть скрыта.

Левая часть панели содержит название и логотип приложения. Если вы нажмете на название или логотип приложения, откроется домашняя страница Консоли OSMP.

В правой части панели отображается следующее:

- Значок уведомления (🔔). Если нажать на значок, откроется панель с уведомлениями.

- Меню вашей учетной записи. Содержит ссылку на справку Kaspersky EDR Expert. В этом меню вы можете просмотреть ваш статус, версию Консоли OSMP, список установленных веб-плагинов управления и выйти из Kaspersky EDR Expert.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окон интерфейса Консоли OSMP. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Изменение языка интерфейса Консоли OSMP

Вы можете выбрать язык интерфейса Консоли OSMP.

Чтобы изменить язык интерфейса:

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.

2. Выберите необходимый язык интерфейса.

Изменение домашней страницы OSMP Console

Домашняя страница отображается после входа в OSMP Console.

По умолчанию раздел **Навигация консоли** установлен как домашняя страница. Если необходимо, вы можете изменить домашнюю страницу.

Чтобы изменить домашнюю страницу:

1. В разделе **Навигация консоли** наведите курсор мыши на элемент, который вы хотите установить в качестве домашней страницы.

2. После того как отобразится значок дома (), нажмите на этот значок.

   Домашняя страница изменена. На экране отобразится соответствующее сообщение. Элемент, выбранный в качестве домашней страницы, отмечен значком дома ().

Разделы **Marketplace** и **Параметры** невозможно установить в качестве домашней страницы.

Добавление и удаление закладок

Вы можете добавить часто используемые разделы OSMP Console в закладки, чтобы быстро получать к ним доступ из раздела **Закладки** в главном меню.

Если вы не добавили ни одного раздела в закладки, раздел **Закладки** не отображается в главном меню.

Вы можете добавить в закладки только те разделы, которые отображают страницы. Например, если вы перейдете в раздел **Управление активами** → **Активы (Устройства)**, откроется страница с таблицей устройств, что означает, что вы можете добавить этот раздел в закладки. Если после выбора раздела в главном меню не отображается окно или элемент, то добавить такой раздел в закладки невозможно.

Чтобы добавить раздел в закладки:

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.

2. После того как значок закладки () отобразится, нажмите на значок.

   Раздел отображается в разделе **Закладки**.

Чтобы удалить раздел из закладок:

1. В главном окне приложения перейдите в раздел **Закладки**.

2. Наведите курсор мыши на раздел, который вы хотите удалить из закладок, и нажмите на значок закладки ( ).

Раздел удален из закладок.

Вы также можете добавлять и удалять разделы из закладок в разделе **Навигация консоли**, наведя на них курсор мыши и нажав на значок закладки ( ). Выбранный элемент будет отмечен значком закладки ( ) и отобразится в разделе **Закладки** главного меню. Если вы хотите удалить элемент из закладок, нажмите на значок закладки ( ).

Раздел **Закладки** отображается только в главном меню. Этот раздел никогда не отображается на странице **Навигация консоли**.

Новая навигация в KEDR

Навигация в KEDR 8.3 существенно отличается от навигации в KEDR 7.1 – изменения указаны в таблице ниже.

Изменения навигации в KEDR

Навигация в KEDR 7.1	Навигация в KEDR 8.3
Мониторинг	**Мониторинг** → **Панель мониторинга** **Мониторинг** → **Панель мониторинга** → **Обнаружение и реагирование**
Алерты	**Мониторинг** → **Алерты**.
Поиск угроз	**Мониторинг** → **Поиск угроз**
Задачи	**Мониторинг** → **История реагирований** **Управление активами** → **Активы (Устройства)** **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**
Политики → **Правила запрета**	**Мониторинг** → **Ресурсы и сервисы** → **Правила запрета**
Политики → **Предустановки**	Недоступно. Рекомендуется использовать плейбуки вместо пресетов.
Пользовательские правила → **TAA**	**Мониторинг** → **Ресурсы и сервисы** → **Правила корреляции**
Пользовательские правила → **IOC**	**Мониторинг** → **Ресурсы и сервисы** → **IOC-правила**
Пользовательские правила → **YARA**	**Мониторинг** → **Ресурсы и сервисы** → **YARA-правила**
Пользовательские правила → **Sandbox**	**Мониторинг** → **Ресурсы и сервисы** → **Правила Sandbox**
Хранение → **Файлы**	**Операции** → **Хранилища** → **Файлы**
Хранение → **Карантин**	**Операции** → **Хранилища** → **Карантин**
Активы	**Управление активами** → **Активы (Устройства)**
Отчеты	**Панель мониторинга** → **Отчеты**
Параметры → **Пользователи** → **Пользователи**	**Пользователи и роли** → **Пользователи и группы** **Параметры** → **Тенанты** → Выбрать тенант → **Права доступа**
Параметры → **Исключения** → **TAA**	Веб-плагин Kaspersky Endpoint Security.
Параметры → **Endpoint Agents** → **Расписание IOC-проверки**	**Параметры** → **Тенанты** → выберите тенант → **Параметры** → **Параметры сканирования** → **Расписание IOC-проверки**
Параметры → **Endpoint Agents** → **Автоматическая отправка файлов в Sandbox**	**Параметры** → **Тенанты** → выберите тенант → **Параметры** → **Параметры сканирования** → **Sandbox**

Навигация в KEDR 7.1	Навигация в KEDR 8.3
Параметры → **Уведомления**	**Параметры** → **Тенанты** → выберите тенант → **Параметры** → **Шаблоны электронных писем**
Параметры → **KSN/KPSN и MDR** → **Участие в KSN/KPSN**	**Параметры** → **Kaspersky Security Network**
Параметры → **KSN/KPSN и MDR** → **Интеграция MDR**	**Мониторинг** → **MDR**
Параметры → **Пароли к архивам**	**Параметры** → **Тенанты** → выберите тенант → **Параметры** → **Параметры сканирования** → **Архивы**
Серверы Sandbox	**Параметры** → **Тенанты** → выберите тенант → **Параметры** → **Серверы Sandbox**

Обнаружение угроз

Kaspersky EDR Expert использует алерты и инциденты в качестве рабочих элементов, которые должны обрабатываться аналитиками.

Разделы **Алерты** и **Инциденты** отображаются в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky EDR Expert.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Работа с алертами

Этот раздел содержит общую информацию об алертах, их свойствах, типичном жизненном цикле и связи с инцидентами. Предоставленные инструкции помогут вам проанализировать таблицу алертов, изменить свойства алертов в соответствии с текущим состоянием жизненного цикла и объединить алерты в инциденты путем связывания или удаления связи алертов.

Раздел **Алерты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky EDR Expert.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Об алертах

Алерт – это событие в ИТ-инфраструктуре организации, которое было отмечено Kaspersky EDR Expert как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуры организации.

Kaspersky EDR Expert формирует алерт, когда EPP-приложение (например, Kaspersky Endpoint Security for Windows) обнаруживает в инфраструктуре определенную активность, соответствующую условиям, заданным в правилах обнаружения.

Алерт создается в течение 30 секунд после возникновения события корреляции KUMA. Если вы ранее настраивали шаблоны уведомлений, вы получите письмо с соответствующим уведомлением по электронной почте.

Также вы можете создать алерт вручную из набора событий.

После детектирования Kaspersky EDR Expert добавляет алерты в таблицу алертов как объекты, которые должны быть обработаны аналитиками. Вы не можете удалить алерты. Их можно только закрыть.

> Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Вы можете управлять алертами как объектами, используя следующие свойства алертов:

- **Статус алерта.**

  Возможные значения: **Новый**, **В обработке**, **Закрыт** или **В инциденте**.

  Статус алерта показывает текущий статус алерта в его жизненном цикле. Вы можете изменить статус по своему усмотрению, за исключением следующих случаев:

  - Вы не можете вернуть закрытые алерты в статус **В обработке**. Закрытые алерты можно вернуть только в статус *Новый*, а затем статус можно изменить на **В обработке**.
  - Вы не можете установить статус **В инциденте** вручную. Алерты получают этот статус, когда они связаны с инцидентом.
  - Вы можете установить статус **Закрыт** только для связанного алерта. Чтобы установить статус **Новый** или **В обработке**, необходимо отменить связь между алертом и инцидентом.

- **Уровень критичности алерта.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Уровень важности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень важности определяется автоматически и не может быть изменен вручную.

- **Ответственный за алерт.**

  Владелец алерта, аналитик, который отвечает за расследование алерта. Вы можете изменить ответственного за алерт в любое время. Невозможно изменить исполнителя закрытых алертов.

Вы можете комбинировать и связывать алерты с более крупными рабочими объектами, называемыми *инцидентами*. Вы можете связать алерты с инцидентами вручную или включить правила для автоматического создания инцидентов и связывания алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему. Когда вы связываете алерт, ни с чем не связанный в текущий момент, с инцидентом, алерт приобретает статус **В инциденте**. Вы можете связать алерт, ни с чем не связанный в текущий момент, с другим инцидентом. В этом случае статус алерта **В инциденте** сохраняется. Вы можете связать с инцидентом не более 200 алертов.

Каждый алерт содержит *детали алерта*, которые содержат всю информацию, относящуюся к алерту. Вы можете использовать эту информацию для исследования алерта, отслеживания событий, предшествующих алерту, просмотра обнаруженных артефактов, затронутых активов или для привязки алерта к инциденту.

Модель данных алерта

Структура алерта представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Assets`).

Алерт

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор алерта (в формате UUID). Значение поля может совпадать со значением `SourceID`.
`ID`	Целое число	Да	Короткий внутренний идентификатор алерта.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан алерт (в формате UUID).
`CreatedAt`	Строка	Да	Дата и время создания алерта (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения алерта (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса алерта (в формате RFC 3339).
`Severity`	Строка	Да	Важность алерта. Возможные значения: • `critical` • `high` • `medium` • `low`
`IntegrationID`	Строка	Да	Идентификатор плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`IntegrationCompatibilityVersion`	Строка	Да	Версия плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`SourceID`	Строка	Нет	Уникальный идентификатор алерта в интегрированном компоненте.
`SourceCreatedAt`	Строка	Нет	Дата и время создания алерта в интегрированном компоненте (в формате RFC 3339).
`FirstEventTime`	Строка	Да	Дата и время первого события телеметрии, связанного с алертом (в формате RFC 3339).
`LastEventTime`	Строка	Да	Дата и время последнего события телеметрии, связанного с алертом (в формате RFC 3339).
`DetectSource`	Строка	Нет	Компонент, который обнаруживает и генерирует алерт.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Состояние`	Строка	Да	Статус алерта. Возможные значения: • `new` • `inProgress` • `inIncident` • `closed`
`StatusResolution`	Строка	Нет	Решение статуса алерта. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`
`IncidentID`	Строка	Нет	Внутренний идентификатор инцидента, связанного с алертом.
`IncidentLinkType`	Строка	Нет	Способ добавления алерта в инцидент. Возможные значения: • `manual` • `auto`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен алерт.

MITRETactics	Массив объектов MITRETactic	Нет	Тактики MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
MITRETechniques	Массив объектов MITRETechnique	Нет	Техники MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
Observables	Массив объектов Observable	Нет	Наблюдаемые объекты, связанные с алертом.
Assets	Массив объектов Asset	Нет	Активы, затронутые алертом.
Rules	Массив объектов Rule	Нет	Сработавшие правила корреляции, на основании которых формируется алерт.
OriginalEvents	Массив объектов	Нет	События, на основании которых формируется алерт.
ExternalRef	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
Extra	Объект	Нет	Данные, связанные с алертом, в формате JSON. Эти данные получены от управляемых приложений "Лаборатории Касперского", когда события преобразуются в алерты. Это поле не используется в интерфейсе.
AdditionalData	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
IsCII	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
Имя	Строка	Да	Название алерта.
Attachments	Массив объектов UnkeyedAttachment	Нет	Вложения, связанные с инцидентом.

Исполнитель

Поле	Тип значения	Требуется	Описание
ID	Строка	Да	Идентификатор учетной записи оператора, которому назначен алерт.
Имя	Строка	Да	Имя оператора, которому назначен алерт.

MITRETactic

Поле	Тип значения	Требуется	Описание
ID	Строка	Да	Идентификатор тактики MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
Имя	Строка	Да	Название тактики MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

MITRETechnique

Поле	Тип значения	Требуется	Описание
ID	Строка	Да	Идентификатор техники MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
Имя	Строка	Да	Название техники MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

Наблюдаемый объект

Поле	Тип значения	Требуется	Описание
`Тип.`	Строка	Да	Тип наблюдаемого объекта. Возможные значения: • `ip` • `md5` • `sha256` • `url` • `domain` • `userName` • `hostName`
`Значение`	Строка	Да	Значение наблюдаемого объекта.
`Details`	Строка	Нет	Дополнительная информация о наблюдаемом объекте.

Правило

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор сработавшего правила.
`Имя`	Строка	Нет	Имя сработавшего правила.
`Уровень важности`	Строка	Нет	Критичности сработавшего правила. Возможные значения: • `critical` • `high` • `medium` • `low`
`Confidence`	Строка	Нет	Уровень доверия сработавшего правила. Возможные значения: • `high` • `medium` • `low`
`Custom`	Логический оператор	Нет	Индикатор того, что алерт основан на пользовательских правилах.

Актив

Поле	Тип значения	Требуется	Описание
`Тип.`	Строка	Да	Тип затронутого актива (устройство или учетная запись). Возможные значения: • `host` • `user`
`ID`	Строка	Да	Идентификатор затронутого актива (устройства или учетной записи).
`Имя`	Строка	Нет	Имя затронутого устройства, с которым связан алерт (если для параметра `Type` выбрано значение `host`). Имя пользователя затронутой учетной записи, связанной с событиями, на основе которых создается алерт (если для параметра `Type` выбрано значение `user`).

`IsAttacker`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакующим.
`IsVictim`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`CIICategory`	Строка	Нет	Категория значимости того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры. Возможные значения: • `notCII` • `ciiWithoutCategory` • `ciiFirstCategory` • `ciiSecondCategory` • `ciiThirdCategory`

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Имя`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Состояние`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Описание`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Просмотр таблицы алертов

Таблица алертов отображается в разделе **Мониторинг** → **Алерты** и предоставляет обзор всех алертов, зарегистрированных в Kaspersky EDR Expert. По умолчанию в таблице отображаются алерты, относящиеся ко всем тенантам, к которым у вас есть права доступа. При необходимости таблицу алертов можно настроить.

Чтобы настроить таблицу алертов, выполните одно из следующих действий:

- Примените фильтр для тенантов:

  a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

     Откроется список тенантов.

  b. Установите флажки рядом с требуемыми тенантами.

- Отфильтруйте данные таблицы алертов одним из следующих методов:
  - Использование основного фильтра:
    a. Нажмите на значок фильтра ( ).
    b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.
  - Фильтрация повторно проверенных алертов:
    a. Нажмите на заголовок столбца **Название**.
    b. Установите флажок **Только повторно проверенные алерты** или **Исключить повторно проверенные алерты**.
  - Использование контекстного фильтра ячейки для быстрого добавления нового условия фильтра:
    a. Найдите ячейку, содержащую значение, которое требуется добавить в качестве условия фильтра. Обратите внимание, что в ячейках некоторых столбцах нет контекстного фильтра.
    b. Нажмите на значение в ячейке.
    c. В открывшемся списке выберите одно из следующих действий:
      - **Добавить в фильтр**, чтобы добавить значение в условие фильтра.
      - **Исключить из фильтра**, чтобы исключить значение из условий фильтрации.
      - **Копировать**, чтобы скопировать значение в буфер обмена.
- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица алертов будет настроена и в ней отобразятся требуемые данные.

В таблице алертов есть следующие столбцы:

- **Зарегистрировано**. Дата и время, когда алерт был добавлен в таблицу алертов.
- **Время обновления**. Дата и время последнего изменения в истории алертов.
- **ID алерта**. Уникальный идентификатор алерта.
- **Статус**. Текущий статус алерта.
- **Тип ссылки инцидента**. Способ добавления алерта в инцидент.
- **Важность**. Важность алерта.
- **Название**. Название алерта.
- **Обнаружено**. Одна или несколько категорий обнаруженных объектов. Например, если решение Kaspersky EDR Expert обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** для этого обнаружения будет указана категория Trojan-Downloader.JS.Cryptoload.ad.

- **Затронутые активы**. Устройства и пользователи, затронутые алертом.

  С момента добавления актива в OSMP требуется приблизительно 2 минуты, пока решение сможет обогащать этим активом события. Например, если вы добавили актив и в течение двух минут произошло корреляционное событие, в созданном алерте такой актив отображаться не будет.

- **Назначен**. Текущий исполнитель алерта.

- **Свойства события**. Артефакты обнаружения, например IP-адреса или MD5-хеши файлов.

- **Подробнее**. Краткая информация об алерте.

- **Статус изменен**. Дата и время последнего изменения статуса алерта.

- **Тенант**. Имя тенанта, в котором зарегистрирован алерт.

- **Внешняя ссылка**. Номер алерта во внешней системе.

- **Объект КИИ**. Индикатор наличия связи алерта с активами, относящимися к объектам КИИ.

- **Технология**. Названия модулей или компонентов, сгенерировавших алерт при проверке.

  Возможные значения в этом столбце:

  - IOA
  - SB (Sandbox)
  - AM (Anti-Malware Engine)
  - IOC
  - YARA
  - KUMA

Особенности агрегации событий в алертах, инициированных правилами IOA

Если Kaspersky EDR Expert создал алерт, инициированный правилом IOA, и то же правило IOA срабатывает в результате других событий на этом или других хостах в тот же день, Kaspersky EDR Expert агрегирует эти события в одном алерте. Если алерт уже закрыт, Kaspersky EDR Expert откроет его повторно. Период агрегации событий заканчивается в 00:00 на следующий день.

Просмотр деталей алерта

Детали алерта – это страница в интерфейсе, которая содержит всю информацию, относящуюся к алерту, включая свойства алерта.

Чтобы просмотреть детали алерта:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. В таблице алертов нажмите на идентификатор требуемого алерта.

   Отображаются детали алерта.

При необходимости можно обновить информацию в деталях алерта, нажав на кнопку обновления (🔄) рядом с названием алерта.

Панель инструментов в верхней части деталей алерта позволяет выполнять следующие действия:

- Изменять значение поля **Внешняя ссылка**
- Назначить алерт аналитику
- Изменить статус алерта
- Связать алерт с инцидентом
- Отменить связь алерта с инцидентом
- Выбрать плейбук
- Создать инцидент и привязать к нему алерт

В зависимости от типа алерта сведения об алерте содержат следующие разделы:

- **Сводная информация**

  В зависимости от типа алерта сводная информация может содержать следующие свойства алерта:

  - **Аналитик**. Аналитик, которому назначен алерт.
  - **Имя**. Название алерта. Если название алерта не указано, это поле не отображается.
  - **Тенант**. Имя тенанта, в котором зарегистрирован алерт.
  - **Активы**. Количество учетных записей пользователей и устройств, связанных с алертом.
  - **Важность**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**. Уровень важности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского".

- **Правила**. Правила, которые сработали для регистрации алерта. Вы можете нажать на значок с многоточием рядом с названием правила, чтобы открыть контекстное меню. Используйте это меню, чтобы узнать больше о правиле, найти алерты или инциденты, которые были зарегистрированы этим же правилом, или выполнить поиск событий, инициировавших правило, в разделе **Поиск угроз** за период между первым и последним событием алерта.

  > Когда в меню вы нажимаете на раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается в той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- **Зарегистрировано**. Дата и время, когда алерт был добавлен в таблицу алертов.
- **Первое событие**. Дата и время первого события, связанного с алертом.
- **Последнее событие**. Дата и время последнего события, связанного с алертом.
- **Внешняя ссылка**. Ссылка на объект во внешней системе (например, ссылка на инцидент Jira). Вы можете нажать на кнопку **Изменить**, чтобы указать внешнюю ссылку. Если алерт был создан из алерта Kaspersky Endpoint Detection and Response alert, ссылка на этот алерт отображается в поле.
- **Связанный с**. Инцидент, к которому привязан алерт.
- **Тактика MITRE**. Тактика или несколько тактик, зарегистрированных в алерте. Вы можете открыть контекстное меню, нажав на имя тактики MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о тактике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о тактике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название тактики MITRE.
- **Техника MITRE**. Техника или несколько техник, зарегистрированных в алерте. Вы можете открыть контекстное меню, нажав на имя техники MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о технике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о технике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название техники MITRE.
- **Правила корреляции**. Правила корреляции, сработавшие для обнаружения угрозы и создания алерта.

- **IOA-правила**. IOA-правила, сработавшие для обнаружения угрозы и создания алерта. Вы можете открыть контекстное меню, нажав на имя IOA-правила. В контекстном меню можно проводить следующие действия:

  - Просмотреть подробную информацию о конкретном IOA-правиле, нажав на кнопку **Открыть свойства**.

  - Просмотреть связанные события, нажав на кнопку **Перейти в Поиск угроз**.

    Выполняется перенаправление в раздел **Поиск угроз**, в котором отображаются только события, отслеживаемые данным правилом IOA. По умолчанию события отображаются за 24 часа. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход.

  - Найти похожие инциденты.

  - Чтобы просмотреть подробную информацию о IOA-правиле в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.

  - Скопировать имя IOA-правила.

- **Технологии**. Технология обнаружения, используемая для обнаружения угрозы.

- **Источник обнаружения**. Источник, от которого поступил обнаруженный объект. Например, если файл был отправлен в Sandbox для проверки с какого-либо устройства, это устройство является источником обнаружения.

- **Дополнительные данные**. Дополнительная информация об алерте. Вы можете изменить значение в этом поле только с помощью плейбука. Поле отображается, если вы добавили значение.

- **Результат проверки**

  В разделе **Результат проверки** содержится информация о проверяемом файле и результатах проверки, по которым был создан алерт.

- **Результаты IOC-проверки**

  В разделе **Результаты IOC-проверки** приводится информация о правилах IOC, сработавших во время проверки.

  По нажатию на название IOC-правила можно просмотреть подробные сведения об этом IOC-правиле.

  По нажатию на кнопку **Посмотреть отчет** в столбце **Результаты проверки** можно просмотреть подробную информацию о результатах проверки, включая сведения о сети и системе, а также о процессах и файлах, задействованных при проверке.

- **Результаты проверки Kaspersky Sandbox**

  Раздел **Результаты проверки Kaspersky Sandbox** содержит информацию о результатах обработки объектов в Sandbox, в том числе:

  - Количество обнаруженных объектов и их типы.

  - Количество извлеченных файлов и их типы.

  - Хеши обнаруженных объектов.

По нажатию на кнопку **Экспорт результатов** можно просмотреть подробную информацию о результатах обработки объектов в операционных системах, доступных в Sandbox, в том числе:

- Диаграммы статистики обнаружений.
- Граф дерева активности объектов.
- Тактики и техники MITRE (см. базу знаний MITRE ATT&CK).
- Список подозрительных действий в операционной системе.
- Скриншоты исполнения файла в операционной системе.
- Системная активность.
- Сетевая активность.

Для просмотра всей информации в окне результатов проверки Sandbox можно переключаться между операционными системами и между результатами, полученными **в режиме быстрой проверки** и **в режиме ведения полного журнала**.

- **Результаты YARA-проверки**

  Раздел **Результатов YARA-проверки** содержит информацию о результатах YARA-проверки на хосте.

  По нажатию на кнопку **Посмотреть отчет** в столбце **Результаты проверки** можно просмотреть подробную информацию о результатах проверки. Для просмотра полной информации в окне результатов проверки YARA можно переключаться между вкладками **Дамп памяти процесса**, **Файлы** и **Условия правила**.

- **Проверяемые файлы**

  В разделе **Проверяемые файлы** приводится информация о проверенных файлах. Для получения дополнительной информации об угрозах, обнаруженных в файлах, на Kaspersky Threat Intelligence Portal, нажмите на название угрозы в столбце **Вердикт**.

- **Подробная информация**

  В разделе **Сведения** можно отслеживать события телеметрии, связанные с алертом.

  В таблице событий отображается результат поиска, который вы определяете с помощью SQL-запроса.

  Панель инструментов таблицы событий позволяет выполнить следующие действия:

  - **Скачать события**. Вы можете нажать на эту кнопку, чтобы загрузить информацию о связанных событиях в CSV-файл (в кодировке UTF-8).
  - **Поиск в разделе Поиск угроз**. Вы можете нажать на эту кнопку, чтобы открыть раздел **Поиск угроз**. Этот раздел позволяет выполнять поиск по всем событиям, связанным с тенантами, к которым у вас есть доступ, а не только по событиям, связанным с текущим алертом. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход.

    По умолчанию открытая таблица событий в разделе содержит все события, произошедшие в период между первым и последним событием в алерте. Например, вы можете запустить поисковый запрос, чтобы найти все события, в которых было задействовано устройство.

    В разделе **Поиск угроз** вы можете вручную связать события с алертами. Это может быть полезно, если вы выясните, что некоторые события относятся к алерту, но не были связаны с алертом автоматически. Дополнительные сведения см. в инструкциях по связыванию или удалению связи событий с алертами.

Вы можете вернуться к деталям инцидента, нажав на кнопку **Исследование алерта** или нажав на кнопку Назад в вашем браузере.

- **Удалить связь с алертом**. Вы можете выбрать событие или несколько событий в таблице и нажать на эту кнопку, чтобы удалить связь выбранных событий с алертом.

- **Активы**

В окне **Активы** можно выполнить следующие действия:

- Просмотреть устройства и пользователей, затронутые алертом или вовлеченные в него.
- Выполните действия по реагированию. Для этого установите флажок рядом с активом, а затем в раскрывающемся списке **Выбрать действие по реагированию** выберите необходимое действие по реагированию.
- Чтобы экспортировать информацию о затронутых активах в CSV-файл, нажмите на кнопку **Экспортировать в CSV**.
- Подключитесь к активу с помощью удаленного терминала. Для этого нажмите на кнопку **Открыть удаленный терминал**.

Таблица активов содержит следующие столбцы:

- **Тип актива**

  Возможные значения: устройство или пользователь.

- **Имя актива**
- **Идентификатор актива**
- **Имеет признаки**

  Возможные значения: атакующий или атакуемый.

- **Статус авторизации**

  Этот параметр применяется только к типу актива – устройство. Статус авторизации устройства определяется KICS for Networks. Вы можете изменить статус авторизации, применив соответствующее действие по реагированию к устройству.

- **Сервер администрирования**

  Сервер администрирования, который управляет устройством.

- **Группа администрирования**

  Группа администрирования, к которой принадлежит пользователь.

- **Категории**

  Категории активов, в которые входит актив.

- **Отправлено в архив**

  Статус объекта в архиве. Возможные значения: Yes или No.

Нажав на имя пользователя или устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.

- Скопировать имя пользователя или имя устройства в буфер обмена.
- Выполнить поиск по имени пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по имени пользователя или идентификатору устройства в других инцидентах.
- Выполнить поиск имени пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после нажатия на имя пользователя или название устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

Нажав на идентификатор пользователя или идентификатор устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.

- Скопировать идентификатор пользователя или идентификатор устройства в буфер обмена.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других инцидентах.
- Выполнить поиск идентификатора пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после нажатия на идентификатор пользователя или идентификатор устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

С момента добавления актива в OSMP требуется приблизительно 2 минуты, пока решение сможет обогащать этим активом события. Например, если вы добавили актив и в течение двух минут произошло корреляционное событие, в созданном алерте такой актив отображаться не будет.

- **Файлы**

  Раздел **Файлы** содержит файлы, полученные в результате действий по реагированию или добавленные вручную в этот алерт. Вы можете загружать, скачивать или удалять файлы, связанные с алертом, или изменять описание файлов.

  Вы можете загружать файлы любого расширения. Допускаются дубликаты имен файлов. Максимальное количество файлов, которые вы можете прикрепить к инциденту, и максимальный общий размер файлов, вы можете указать в конфигурационном файле.

  Ограничения по умолчанию:

  - Количество файлов не может превышать 100 на один алерт.
  - Общий размер файла не может превышать 25 МБ на один алерт.

  Чтобы загрузить файлы, нажмите на кнопку **Загрузить** и выберите один или несколько файлов. Если вы попытаетесь загрузить файлы, превышающие ограничения, появится панель **Загрузка файлов** с предупреждающим сообщением. В этой панели вы можете удалять файлы из очереди загрузки до тех пор, пока не исчезнет предупреждающее сообщение, и нажать на кнопку **Загрузить**, чтобы загрузить файлы. Если вы проигнорируете предупреждающее сообщение, загрузка не будет выполнена, а в списке файлов появятся файлы, которые не удалось загрузить, со значком предупреждения рядом с именами файлов.

  После нажатия на кнопку **Загрузить** панель закрывается, и загруженный файл отображается в таблице файлов в сведениях об алерте и в главном меню приложения в разделе **Файлы**. При загрузке большого файла или нескольких файлов вам нужно обновить таблицу, чтобы в ней отображались новые файлы. Если загрузка файла выполняется, в столбце **Имя или полный путь** отображается индикатор загрузки, а в столбце **Размер** отображается размер уже загруженного файла.

  Нажмите на файл, чтобы открыть панель **Изменить файл**, на которой отображаются сведения о файле. В этой панели вы можете изменить описание файла.

  Используйте флажки для выбора файла или нескольких файлов. Выберите один или несколько файлов и нажмите на кнопку **Скачать**, чтобы скачать архив файлов в формате ZIP. Архив защищен паролем *infected*. Выберите файл или несколько файлов и нажмите на кнопку **Удалить**, чтобы удалить выбранные файлы.

  Для загрузки и удаления файлов и изменения описаний файлов требуется право **Запись** в функциональной области **Алерты и инциденты**. Для возможности скачивать файлы требуется право на **Чтение** в функциональной области **Алерты и инциденты**.

- **Наблюдаемые объекты**

  В разделе **Наблюдаемые объекты** вы можете:

  - Просмотреть наблюдаемые объекты, связанные с алертом.
  - Экспортировать информацию о связанных наблюдаемых объектах в CSV-файл, нажав на кнопку **Экспортировать в CSV**.
  - Выполнить поиск в таблице наблюдаемых объектов по данным из столбца **Значение**.

    Для этого в строке поиска начните вводить данные искомого наблюдаемого объекта. При отсутствии совпадений со значениями наблюдаемых объектов из столбца **Значение** отображается пустая таблица.

  Наблюдаемые объекты могут включать:

  - MD5-хеш
  - URL
  - Имя домена

- SHA256
- UserName
- HostName
- Локальный IP-адрес
- Удаленный IP-адрес

  Следующие частные IP-адреса не включены в наблюдаемые объекты, связанные с алертом:
  От 10.0.0.0 до 10.255.255.255 с маской подсети 255.0.0.0 или /8.
  От 172.16.0.0 до 172.31.255.255 с маской подсети 255.240.0.0 или /12.
  От 192.168.0.0 до 192.168.255.255 с маской подсети 255.255.0.0 или /16.
  От 100.64.0.0 до 100.127.255.255 с маской подсети 255.192.0.0 или /10.

  Чтобы включить частные IP-адреса в наблюдаемые данные, выполните следующие команды на устройстве администратора:

  ```
  k0s kubectl -n irp set env deploy/transformer -c transformer
  OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
  ```

  ```
  k0s kubectl -n irp set env deploy/incident -c incident
  OSMP_FILTER_PRIVATE_IPS_DISABLED=true
  ```

- Локальный порт
- Удаленный порт
- Идентификатор системного процесса
- Уникальный PID
- Полное имя файла

Нажав на ссылку в столбце **Значение**, вы можете:

- Поиск наблюдаемого значения в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после перехода по ссылке в столбце **Значение** вы выбираете в меню раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- Выполнить поиск по значению наблюдаемого объекта в других алертах.

- Выполнить поиск по значению наблюдаемого объекта в других инцидентах.
- Скопировать значение наблюдаемого объекта в буфер обмена.

Панель инструментов этого раздела содержит следующие кнопки:

- **Запросить статусы Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). В результате информация обновляется в столбце **Статус обновления**. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Обогатить данные Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию обо всех перечисленных наблюдаемых объектах из Kaspersky TIP. В результате информация обновляется в столбце **Обогащение**. Используйте ссылку в столбце **Обогащение**, чтобы открыть полученные сведения об обогащении наблюдаемого объекта. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Выбор действий по реагированию**. Чтобы выполнить действия по реагированию, установите флажок рядом с наблюдаемым объектом и в выпадающем списке **Выбор действий по реагированию**, выберите необходимые действия по реагированию:
  - **Запустить**. Используйте эту кнопку, чтобы запустить приложение с указанными параметрами.
  - **Получить файл**. Используйте эту кнопку, чтобы скачать архив с файлом на ваше устройство.
  - **Заблокировать (NGFW)**. Используйте эту кнопку, чтобы добавить IP-адрес, URL или домен в список запрещенных на сетевых устройствах.
  - **Управлять службами**. Используйте эту кнопку, чтобы удаленно запускать, останавливать, приостанавливать, возобновлять или удалять службу на устройстве. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Прервать процесс**. Используйте эту кнопку, чтобы прервать процессы, связанные с файлом. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Удалить файл**. Используйте эту кнопку, чтобы удалять файлы.
  - **Поместить на карантин**. Используйте эту кнопку, чтобы переместить устройство, на котором находится файл, на карантин. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Добавить правило запрета**. Используйте эту кнопку, чтобы добавить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Удалить правило запрета**. Используйте эту кнопку, чтобы удалить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- **Похожие закрытые алерты**

  В разделе **Похожие закрытые алерты** вы можете просмотреть список закрытых алертов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Похожие закрытые алерты могут помочь вам изучить текущий алерт.

  С помощью списка вы можете оценить степень сходства текущего алерта и других алертов. Сходство рассчитывается следующим образом:

  Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном алерте, "T" – общее количество артефактов в текущем алерте.

Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным алертом. Если сходство равно 0%, текущий и аналогичный алерт полностью различаются. Алерты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор алерта открываются детали алерта.

Настройка списка похожих закрытых алертов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте алерты, выбрав период, за который были обновлены алерты. По умолчанию список содержит алерты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать алерты в порядке возрастания или убывания.

- **Подобные инциденты**

В разделе **Подобные инциденты** вы можете просмотреть список инцидентов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Подобные инциденты могут помочь вам решить, может ли текущий алерт быть связан с существующим инцидентом.

С помощью списка вы можете оценить степень сходства текущего алерта и инцидентов. Сходство рассчитывается следующим образом:

Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном инциденте, "T" – общее количество артефактов в текущем алерте.

Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным инцидентом. Если сходство равно 0%, текущий алерт и схожий инцидент полностью различаются. Инциденты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор инцидента открывается подробная информация об инциденте.

Настройка списка похожих инцидентов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте инциденты, выбрав период, за который были обновлены инциденты. По умолчанию список содержит инциденты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать инциденты в порядке возрастания или убывания.

- **Комментарии**

  В разделе **Комментарии** вы можете оставлять комментарии, связанные с алертом. Например, вы можете написать комментарий о результатах расследования или при изменении свойств алерта, таких как исполнитель или статус алерта.

  Чтобы сохранить комментарий, нажмите на клавишу **`Enter`**. Чтобы начать новую строку, нажмите на клавиши **`Shift + Enter`**. Чтобы изменить или удалить свой комментарий, используйте кнопки в правом верхнем углу.

  Вы можете редактировать и удалять собственные комментарии только в течение определенного промежутка времени после того, как оставите их. По умолчанию задан период в 15 минут.

  Если вы хотите изменить этот промежуток, выполните следующую команду на хосте администратора:

  ```
  k0s kubectl -n irp set env deploy/comment -c comment
  OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
  ```

  где `N` – промежуток времени, а `x` – единица измерения: `h` (часы) или `m` (минуты).

  Комментарии других пользователей невозможно изменить или удалить. Для возможности оставлять комментарии требуется право на **Запись** в функциональной области **Алерты и инциденты**.

- **История**

  В разделе **Журнал изменений** вы можете отслеживать изменения, внесенные в алерт как в объект:

  - изменение статуса алерта;
  - изменение исполнителя алерта;
  - связь алерта с инцидентом;
  - удаление связи между алертом и инцидентом;
  - загрузка файла в алерт;
  - удаление файла из алерта.

В разделе **История реагирований** вы можете просмотреть действия по реагированию, выполненные вручную, а также действия, выполненные в рамках плейбука. Таблица содержит следующие столбцы:

- **Время**. Время возникновения события.
- **Запущено**. Имя пользователя, запустившего действие по реагированию.
- **События**. Описание события.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
- **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **Запущено** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.
- **Плейбук**. Название плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

Назначение алертов аналитикам

Как объект, алерт должен быть передан аналитику SOC или группе пользователей для проверки и возможного расследования. Вы можете автоматически назначать алерты аналитикам в выбранной группе пользователей. Подробнее см. раздел Настройка автоматического назначения алертов и инцидентов.

Вы можете изменить исполнителя активного алерта в любое время. Вы не можете изменить исполнителя закрытого алерта.

Алерты можно назначить только аналитикам или группе пользователей, имеющим право на чтение и изменение алертов и инцидентов.

Чтобы назначить алерт или несколько алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. Установите флажки напротив алертов, которые нужно назначить.

   Вам нужно выбрать только алерты, обнаруженные в одном тенанте. Иначе кнопка **Назначить** будет неактивна.

   Также вы можете назначить алерт аналитику или группе пользователей из деталей алерта. Чтобы открыть детали алерта, перейдите по ссылке с нужным идентификатором алерта.
3. Нажмите на кнопку **Назначить**.
4. В открывшемся окне **Назначить аналитику** выберите пользователя или группу пользователей, которым нужно назначить алерты.
5. Начните вводить имя аналитика или группы пользователей, а затем выберите исполнителя из списка.

   Если вы хотите отменить назначение алертов, выберите **Не назначен**.

   Вы можете выбрать **Не назначен** для всех алертов, кроме алертов со статусом **Закрыт**.
6. Нажмите на кнопку **Назначить**.

Алерты назначены.

Также можно назначить алерт с помощью плейбуков.

Изменение статуса алерта

Как объект, алерт имеет статус, который показывает текущий статус алерта в его жизненном цикле.

Вы можете изменять статусы алертов для своих алертов или алертов других аналитиков, только если у вас есть право доступа для чтения и изменения алертов и инцидентов.

Если статус алерта изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого алерта вручную.

Алерт может иметь один из следующих статусов:

- **Новое.**

  Когда Kaspersky EDR Expert регистрирует новый алерт, он имеет статус *Новый*. Вы можете изменить статус на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *Закрыт* и у алерта нет исполнителя, оно автоматически назначается вам.

- **В обработке.**

  Этот статус означает, что аналитик начал работу над алертом. Статус *В обработке* может быть изменен на *Новое* и *Закрыто*.

- **Закрыто.**

  Истинно положительные алерты должны быть связаны с инцидентами и расследоваться в рамках инцидентов. Когда вы закрываете инцидент, связанные алерты также переходят в статус *Закрыт*. Вы закрываете несвязанный алерт только как ложное срабатывание или как алерт с низким приоритетом. Когда вы закрываете алерт, вам нужно выбрать решение.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый алерт в работу, измените его статус следующим образом: *Закрыт → Новый → В обработке*.

  Когда вы закрываете алерт, связанный с инцидентом, автоматически удаляется связь с инцидентом. Если алерт, который вы собираетесь закрыть, никому не назначен, он автоматически назначается аналитику, который закрывает алерт.

- **В инциденте.**

  Этот статус назначается алерту при привязке к инциденту. Этот статус нельзя выбрать вручную. Статус *Закрыто* может быть назначен только привязанному алерту. Чтобы сменить этот статус на *Новое* или *В обработке*, необходимо сначала отменить связь алерта с инцидентом.

Чтобы изменить статус одного или нескольких алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив алертов, статус которых вы хотите изменить.
   - Перейдите по ссылке с идентификатором алерта, статус которого вы хотите изменить.

     Откроется окно **Детали алерта**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

   > Если вы измените статус алерта на *Закрыт* и этот алерт содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.

5. Нажмите на кнопку **Сохранить**.

Статусы выбранных алертов будут изменены.

Если алерт добавлен на граф расследования, вы также можете изменить статус алерта на графе.

Также статус алерта можно изменить с помощью плейбуков.

Создание алертов вручную

Вы можете создать алерт вручную из набора событий. Вы можете использовать эту функцию для проверки гипотетического инцидента, который не был обнаружен автоматически.

> Если алерт создан вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого алерта вручную.

Чтобы создать алерт вручную:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.
2. Выберите события, для которых вы хотите создать алерт. События должны принадлежать одному тенанту.
3. Нажмите на кнопку **Создать алерт**.

   Откроется окно с созданным алертом, и вы получите соответствующее уведомление по электронной почте, если шаблоны уведомлений настроены. Значение поля **Важность** соответствует максимальной критичности среди выбранных событий.

Алерты, созданные вручную, имеют пустое значение **Правила** в таблице **Мониторинг** → **Алерты**.

Связь алертов с инцидентами

Вы можете связать один или несколько алертов с инцидентом, по следующим причинам:

- Несколько алертов можно интерпретировать как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае алерты в инциденте можно исследовать как отдельную проблему. Вы можете связать с инцидентом до 200 алертов.
- Один алерт может быть связан с инцидентом, если он определен как истинно положительный.

Вы можете связать алерт с инцидентом, если он имеет любой статус отличный от *Закрыт*. Алерт теряет свой текущий статус и приобретает статус *В инциденте* при связывании с инцидентом. Если вы связываете алерты, которые в настоящее время связаны с другими инцидентами, удаляется связь алертов с текущими инцидентами, так как алерт может быть связан только с одним инцидентом.

> Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту.

Алерты могут быть связаны с инцидентом вручную или автоматически.

Связывание алертов вручную

Чтобы связать алерты с существующим или новым инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. Установите флажки рядом с событиями, которые требуется связать с инцидентом.
3. Если вы хотите связать алерты с существующим инцидентом:
   a. Нажмите на кнопку **Связать с инцидентом**.
   b. Выберите инцидент, с которым нужно связать алерты.

   Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Связать с инцидентом** в панели инструментов.
4. Если вы хотите связать алерты с новым инцидентом:
   a. Нажмите на кнопку **Создать инцидент**.
   b. Заполните свойства нового инцидента: имя, исполнитель, приоритет и описание.

   Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Создать инцидент** в панели инструментов.
5. Нажмите на кнопку **Сохранить**.

Выбранные алерты связаны с существующим или новым инцидентом.

Автоматическая привязка алертов

Если вы хотите, чтобы алерты автоматически связывались с инцидентом, вам нужно настроить правила сегментации.

Удаление связи алертов с инцидентами

Вам может потребоваться удалить связь между алертом и инцидентом, например, если анализ и расследование алертов показали, что алерт не связан с другими алертами в инциденте. При удалении связи алерта с инцидентом Kaspersky EDR Expert выполняет следующие действия:

- Обновляет все данные, связанные с инцидентом, чтобы отразить, что алерт больше не относится к инциденту. Например, вы можете просмотреть изменения в деталях инцидента.
- Сбрасывает статус несвязанных алертов на *Новый*.

Чтобы удалить связь алерта с инцидентом:

1. Откройте детали алерта.
2. Нажмите на кнопку **Удалить связь с инцидентом** в панели инструментов.

   Откроется окно **Удалить связь с алертами**.
3. Если вы хотите сменить исполнителя, выберите **Назначить алерты** и укажите нового исполнителя.
4. Если вы хотите добавить комментарий, укажите его в разделе **Комментарий**. Указанный вами комментарий отображается в столбце **Сведения** в разделе **История**.

Для выбранных алертов удалена связь с инцидентом.

Связывание событий с алертами

Если во время расследования вы обнаружили событие, связанное с исследуемым алертом, вы можете связать это событие с алертом вручную.

> Вы можете связать событие с алертом, если он имеет любой статус отличный от **Закрыт**.

Чтобы привязать событие к алерту:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. В списке алертов перейдите по ссылке с идентификатором алерта, с которым вы хотите связать событие.

   Откроется окно **Детали алерта**.
3. Перейдите в раздел **Подробнее** и нажмите на кнопку **Найти в разделе Поиск угроз**.

   Откроется раздел **Поиск угроз**. По умолчанию таблица событий содержит события, связанные с выбранным алертом.

   > Таблица событий содержит только события, связанные с тенантами, к которым у вас есть доступ.
4. В верхней части окна откройте первый раскрывающийся список и выберите **Хранилище**.
5. Откройте третий раскрывающийся список и укажите период.

   Вы можете выбрать предопределенные периоды относительно текущей даты и времени и указать необходимый период, используя поля **Начало периода** и **Окончание периода** или выбрав даты в календаре.
6. Нажмите на кнопку **Выполнить запрос**.
7. В обновленном списке событий выберите событие, которое вы хотите связать с алертом и нажмите на **Связать с алертом**.

Выбранные события привязаны к алерту.

Удаление связи событий с алертами

Вам может потребоваться удалить связь между событием и алертом, например, если анализ и расследование событий показали, что событие не связано с алертами.

Чтобы удалить связь события с алертом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. В списке алертов перейдите по ссылке с идентификатором алерта, для которого вы хотите удалить связь с событием.

   Откроется окно **Детали алерта**.
3. В разделе **Подробнее** выберите события, для которых вы хотите удалить связь, а затем нажмите на кнопку **Удалить связь с алертом**.

Для выбранных событий удалена связь с алертом.

Поиск событий, связанных с импортированным алертом IOA

Вы можете искать события, связанные с алертом, импортированным из KEDR 7.1.

> Этот сценарий работает только в том случае, если данные телеметрии были перенесены из KEDR 7.1 в OSMP.

Для поиска событий, связанных с алертом:

1. Откройте требуемую страницу деталей алерта.

   Требуемый алерт можно найти по дате его создания и отсутствию каких-либо событий в теле алерта.
2. Запомните или сохраните любым удобным способом диапазон дат события алерта (поля **Первое событие** и **Последнее событие** в разделе **Описание**).
3. В разделе **Описание** нажмите на имя IOA-правила в поле **IOA-правила** и выберите **Открыть свойства**.

   Откроется страница **IOA-правила**.
4. На странице IOA-правил нажмите кнопку **Поиск в разделе Поиск угроз**.

   Откроется раздел **Поиск угроз**.

5. Укажите диапазон дат события из шага 2 данной процедуры:

   a. Нажмите на раскрывающийся список временного периода и введите даты в поля **От** и **До**. Формат даты и времени зависит от параметров вашего браузера.

      Вы также можете выбрать дату в календаре. В этом случае в поле **От** будет автоматически указано значение 00:00:00.000, а в поле **До** – значение 23:59:59.999.

   b. Нажмите на кнопку **Применить**.

6. Нажмите на кнопку **Выполнить запрос**.

События, связанные с алертом, будут отображаться в таблице **События**.

Работа с алертами на графе расследования

На графе расследования вы можете выполнять следующие действия с алертами:

- Добавлять алерт на граф.
- Скрывать алерт с графа.
- Просматривать детали алерта, выбрав соответствующий элемент из контекстного меню узла алерта.
- Изменять статус алерта.
- Просматривать события, связанные с алертом.
- Просматривать активы, связанные с алертом.
- Просматривать наблюдаемые объекты, связанные с алертом.

Добавление алертов на граф расследования

Вы можете добавить алерт на граф расследования одним из следующих способов:

- Из общей таблицы алертов, которая открывается при нажатии на кнопку **Добавить алерт** на графе расследования. Вам нужно установить флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажать на кнопку **Показать на графе**.
- Из таблицы похожих алертов.

Чтобы добавить алерты на граф расследования из таблицы похожих алертов:

1. Выполните одно из следующих действий:

   - Если на графе расследования у вас есть актив, наблюдаемый объект или правило сегментации, нажмите на его узел, а затем в контекстном меню выберите пункт **Найти похожие алерты**.
   - Если на графе расследования у вас есть событие, нажмите на его узел, а затем в контекстном меню выберите пункт **Просмотреть информацию**. В открывшемся окне нажмите на кнопку **Показать на графе**.

- Если на графе расследования у вас есть алерт, нажмите на его узел и в контекстном меню выберите пункт **События**. В таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

- На графе расследования нажмите на кнопку **Поиск угроз**, а затем в общей таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

Отобразится таблица похожих алертов.

2. Установите флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты будут добавлены на граф расследования.

Скрытие алертов на графе расследования

Вы можете скрыть алерты на графе расследования одним из следующих способов:

- Нажать на узел алерта и в контекстном меню выбрать пункт **Скрыть**.

- С помощью таблицы алертов.

Чтобы скрыть алерты на графе с помощью таблицы алертов:

1. Выполните одно из следующих действий:

   - В панели инструментов в верхней части графа расследования нажмите на кнопку **Добавить алерт**.

   - Если на графе отображаются узлы наблюдаемых объектов, активов или событий, нажмите на узел, для которого вы хотите добавить алерт, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

   Отобразится таблица алертов.

2. Установите флажки рядом с алертами, которые вы хотите скрыть на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты и их ссылки будут скрыты на графе расследования. Связанные узлы останутся на графе расследования.

Изменение статуса алерта

Чтобы изменить статус алерта:

1. Нажмите на узел алерта и в контекстном меню выберите пункт **Изменить статус**.
2. В открывшейся панели **Смена статуса**, выберите статус и нажмите на кнопку **Сохранить**.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

Статусы выбранных алертов будут изменены.

Просмотр событий, связанных с алертом

Чтобы просмотреть события, связанные с алертом, выполните одно из следующих действий:

- Нажмите на цифру рядом с узлом алерта, события которого вы хотите отобразить. Цифра показывает количество событий, связанных с алертом.
- Нажмите на узел алерта, события которого вы хотите отобразить, и в контекстном меню выберите пункт **События**.

Если вы хотите добавить события из таблицы на граф расследования, установите флажки рядом с событиями и нажмите на кнопку **Показать на графе**.

Если вы хотите скрыть события на графе расследования, установите флажки рядом с событиями и нажмите на кнопку **Скрыть на графе**.

Просмотр активов, связанных с алертом

Чтобы просмотреть активы, связанные с алертом, нажмите на узел алерта.

В контекстном меню цифры рядом с элементами **Устройства** и **Пользователи** показывают количество устройств и пользователей, связанных с алертом.

Если вы хотите добавить устройства или пользователей на граф расследования, выберите соответствующий пункт меню.

Просмотр наблюдаемых объектов, связанных с алертом

Чтобы просмотреть наблюдаемые объекты, связанные с алертом, нажмите на узел алерта и в контекстном меню выберите пункт **События**.

В открывшемся меню цифры рядом с элементами показывают количество наблюдаемых объектов, связанных с алертом.

Если вы хотите добавить наблюдаемый объект (например, **Хеш**, **Домен**, **IP-адрес**) на граф расследования, выберите соответствующий пункт меню.

Добавление IOA-правила в исключения

Если вы не хотите, чтобы генерировались алерты для событий, сформированных в результате обычной для вашей организации активности активов, вы можете добавить IOA-правило в исключения.

Чтобы добавить IOA-правило в исключения из таблицы алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. Нажмите на значок фильтра.
3. На вкладке **Фильтры** укажите и примените критерий фильтра **Обнаружено** для нужного IOA-правила.
4. В таблице алертов нажмите на идентификатор алерта.

   Отображаются детали алерта.
5. В разделе **Сводная информация** нажмите имя IOA-правила.
6. В панели IOA-правил нажмите **Добавить в исключения**.

   Откроется панель **Добавить в исключения**.
7. На панели **Добавить в исключения** выберите политику или профиль, чтобы добавить IOA-правило в исключение. Нажмите на кнопку **Далее**.
8. Укажите свойства правила исключения и нажмите **Добавить**.

   IOA-правило добавлено в исключения.

Чтобы просмотреть и изменить список исключений IOA для политики:

1. В главном окне приложения перейдите в раздел **Политики**.
2. Нажмите на нужную политику.
3. Выберите вкладку **Параметры приложения**. В разделе **Общие параметры** выберите **Параметры телеметрии**.

   На вкладке **телеметрии EDR Expert (on-premises)** на вкладке **Общие исключения** отображаются исключения IOA.

   - Чтобы выключить правило исключений, выключите переключатель **Статус**.
   - Чтобы удалить правило исключений, установите флажок рядом с правилом исключений и нажмите **Удалить**.
   - Чтобы просмотреть сведения о правиле исключений, нажмите на имя правила исключений.

Управление правилами агрегации

В этом разделе содержится общая информация о правилах агрегации и приведены инструкции о том, как создавать, изменять, дублировать, копировать для другого тенанта и удалять правила агрегации.

Чтобы управлять правилами агрегации, вам нужно иметь одну из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC.

Правила агрегации позволяют вам объединять повторяющиеся события других решений "Лаборатории Касперского" в алерты Open Single Management Platform. Алерты либо связаны с существующими инцидентами, либо формируют новые инциденты.

Вы можете создавать правила агрегации и управлять ими в разделе **Мониторинг** → **Ресурсы и сервисы** → **Правила агрегации**. Правила агрегации отображаются в виде таблицы. Чем выше находится правило в таблице правил агрегации, тем выше его приоритет. Если вы хотите изменить приоритет правила агрегации, вам нужно перетащить правило, нажав на значок (⠿).

Для унаследованных правил вы можете изменить приоритет только в родительском тенанте. В дочернем тенанте приоритет унаследованных правил всегда выше, чем приоритет правил, созданных в дочернем тенанте. Также в унаследованных правилах порядок приоритета такой же как и в родительском тенанте.

Также таблица содержит предустановленное правило агрегации, созданное экспертами "Лаборатории Касперского". Это правило объединяет события, для которых было активировано одно и то же правило корреляции в течение стандартного интервала агрегации (30 секунд).

Вы не можете удалить предустановленное правило агрегации, но вы можете его изменить. По умолчанию правило включено.

По умолчанию предопределенные правила создаются для всех тенантов, и наследование для них выключено. Если вы включите наследование для правила родительского тенанта, соответствующее правило дочернего тенанта будет перезаписано параметрами родительского тенанта. Если вы выключите наследование, правило родительского тенанта будет удалено. Так как тенант не может существовать без предустановленных правил, для дочернего тенанта будет автоматически создано локальное предопределенное правило.

Правила агрегации обрабатываются последовательно в соответствии с указанным приоритетом. При выполнении условия, заданного в разделе **Триггер**, правило агрегации срабатывает и поиск других подходящих правил агрегации продолжается. Поиск останавливается только после обработки всех правил в таблице.

Ограничения, связанные с технологиями обнаружения

В зависимости от технологии обнаружения существуют некоторые ограничения на агрегацию алертов:

- Обнаружение YARA, Sandbox и вредоносного ПО в файле:
  - Вы можете агрегировать обнаружения найденных с помощью этих технологий в одном файле.
  - Вы не можете добавлять обнаружение IOA или результаты IOC-проверки или сканирования YARA.

- Обнаружение IOA:
  - Вы можете объединить в один алерт обнаружения, найденные одним или разными IOA-правилами.
  - Вы не можете добавлять обнаружения, найденные с помощью других технологий.
- IOC-проверки:
  - Вы можете агрегировать результаты IOC-проверки (например, обнаружения по одному и тому же IOC-правилу, по разным IOC-правилам, на одном и том же или на разных устройствах).
  - Вы не можете добавлять обнаружения, найденные с помощью других технологий.
- Сканирования YARA:
  - Вы можете агрегировать результаты сканирования YARA (например, обнаружения по одному и тому же YARA-правилу, по разным YARA -правилам, на одном и том же или на разных устройствах).
  - Вы не можете добавлять обнаружения, найденные с помощью других технологий.

Создание правил агрегации

Правила агрегации помогают вам объединять повторяющиеся события других решений "Лаборатории Касперского" в алерты Open Single Management Platform.

Чтобы создать правила агрегации, вам нужно иметь одну из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC.

Чтобы создать правило агрегации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Агрегация алертов**.

   Откроется таблица правил агрегации.

2. Нажмите на кнопку **Создать**.

   Откроется окно **Создать правило агрегации**.

3. В поле **Статус** активируйте правило агрегации, которое вы хотите создать.

   По умолчанию правило выключено.

4. В поле **Тенант-владелец** укажите тенант, которому будет принадлежать правило агрегации.

5. В поле **Имя** укажите название правила агрегации.

   Имя правила должно быть уникальным.

6. В поле **Максимум событий в алерте** укажите максимальное количество событий, объединенных в алерте.

   Значение должно быть от 1 до 100. Значение по умолчанию – 100.

7. В поле **Интервал агрегации** укажите интервал поиска в минутах или секундах.

   Максимальное значение – 1500 секунд. Значение по умолчанию – 30.

8. При необходимости в поле **Унаследовано** измените параметры наследования.

   По умолчанию правила наследуются от родительского тенанта всеми дочерними тенантами по иерархии. Вы можете выключить наследование, выбрав **Только текущий тенант** или указать тенанты, которые должны наследовать правило, нажав **Заданные тенанты**, а затем выбрав тенанты из раскрывающегося списка.

   > Вы можете указать только тенантов, для которых вам назначена одна из следующих ролей XDR: Главный администратор, администратор тенанта или администратор SOC.
   > Изменение параметров наследования или приоритета правил, а также дублирование или удаление унаследованных правил возможно только из родительского тенанта. Статус унаследованного правила может быть изменен как из родительского, так и из дочернего тенанта.

   В дочернем тенанте приоритет унаследованных правил всегда выше, чем приоритет правил, созданных в дочернем тенанте. Также в унаследованных правилах порядок приоритета такой же как и в родительском тенанте. При дублировании унаследованного правила его область действия также дублируется. При копировании унаследованного правила на другой тенант область действия правила не копируется.

9. В разделе **Название алерта** укажите выражение jq, определяющее шаблон, который будет использоваться при создании имени нового алерта. Это выражение также используется для объединения событий в алерт.

   По умолчанию указано следующее выражение: `([.Rules[]?.Name // empty] | sort | join(","))`

   При создании нового алерта название генерируется из значений полей указанных в шаблоне.

   При необходимости вы можете скопировать выражение jq для раздела **Название алерта** из другого правила агрегации. Для этого нажмите на кнопку **Копировать из другого правила**.

   Пример выражения jq для раздела Название алерта

   ```
   if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Brute force admin" else "Brute force not admin" end
   ```

10. В разделе **Триггер** укажите выражение jq, которое определяет условие для создания алерта из события.

    При необходимости вы можете скопировать выражение jq для раздела **Триггер** из другого правила агрегации. Для этого нажмите на кнопку **Копировать из другого правила**.

    Пример выражения jq для раздела Триггер

    ```
    .AggregationID | startswith("bruteforce_DestinationUserName")
    ```

11. При необходимости в поле **Описание** укажите описание правила агрегации.

12. Нажмите на кнопку **Создать**.

    Правило агрегации создано.

По умолчанию правило агрегации создается с наименьшим приоритетом. Чтобы изменить приоритет правила агрегации, в таблице правил агрегации перетащите правило, нажав на его имя. Чем выше находится правило в таблице правил агрегации, тем выше его приоритет.

Изменение правил агрегации

Вы можете изменить параметры правила агрегации.

> Для унаследованных правил в дочернем тенанте можно менять только их статус. Если вы хотите изменить другие их параметры, это нужно будет сделать из родительского тенанта, после чего изменения будут распространены на дочерние тенанты.

Чтобы изменить правило агрегации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила агрегации**.
2. В таблице правил агрегации нажмите на имя правила агрегации, которое вы хотите изменить.
3. В открывшемся окне **Изменить правило агрегации** измените параметры правила агрегации. Дополнительные сведения о свойствах правила, которые вы можете изменить, см. в разделе Создание правил агрегации.
4. Нажмите на кнопку **Применить**.
5. Если вы хотите изменить приоритет правила агрегации, в таблице правил агрегации перетащите правило, нажав на его имя.

   Чем выше находится правило в таблице правил агрегации, тем выше его приоритет.

Свойства правила агрегации изменены и сохранены.

Копирование правил агрегации в другой тенант

Вы можете скопировать существующее правило агрегации другому тенанту.

> Если иерархия экземпляров OSMP построена, вы можете копировать правила только внутри экземпляра.

Чтобы скопировать правила агрегации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила агрегации**.
2. В таблице правил агрегации выберите правила, которые вы хотите скопировать и нажмите на кнопку **Копировать в тенант**.
3. Выберите один или несколько целевых тенантов и нажмите на кнопку **Копировать**.

4. Если целевой тенант содержит правило агрегации с таким же именем, откроется окно **Перезаписать или переименовать правила агрегации?**:

   - Если вы хотите удалить ранее созданное правило для целевого тенанта и заменить его правилом, которое вы хотите скопировать, нажмите на кнопку **Перезаписать**.

   - Если вы хотите сохранить ранее созданное правило и скопировать указанное правило с добавлением (копия) к его названию, нажмите **Копировать и переименовать**.

   Если вы копируете унаследованное правило, а у целевого тенанта уже есть правило с таким же именем, оно не будет перезаписано. Вам нужно изменить имя правила, которое вы копируете. Также унаследованные правила копируются со своим статусом, но без области действия.

   > При нажатии на кнопку закрытия (×) окно закрывается, а правила агрегации, имена которых совпадают с именам в целевых тенантах, не копируются. Если на шаге 2 вы также выбрали правила агрегации, которых нет в целевых тенантах, такие правила копируются.

Правила агрегации копируются другому тенанту или тенантам.

Удаление правил агрегации

Вы можете удалить одно или несколько правил агрегации сразу.

Если правило агрегации было унаследовано, его можно удалить только из родительского тенанта.

> Удалить предустановленное правило агрегации невозможно. Поскольку тенант не может существовать без предустановленного правила, после его удаления будет автоматически создано локальное предустановленное правило.

Чтобы удалить правила агрегации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила агрегации**.

2. В таблице правил агрегации выберите одно или несколько правил агрегации, которые вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В диалоговом окне нажмите на кнопку **Удалить**.

   Правило агрегации удалено.

Работа с инцидентами

В этом разделе содержится общая информация об инцидентах, их свойствах, типичном жизненном цикле и связи с алертами. В этом разделе также приведены инструкции по созданию инцидентов, анализу таблицы инцидентов, изменению свойств инцидентов в соответствии с текущим состоянием в жизненном цикле и объединению инцидентов.

Раздел **Инциденты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky EDR Expert.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор, Взаимодействие с дочерними инцидентами.

Об инцидентах

Инцидент – это контейнер обнаружений, который обычно указывает на истинно положительную проблему в ИТ-инфраструктуре организации. Инцидент может содержать один или несколько алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему.

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. После создания инцидента вы можете связать алерты с ним. Вы можете связать с инцидентом до 200 алертов.

После создания инцидентов Kaspersky EDR Expert добавляет их в таблицу инцидентов как объекты, которые должны быть обработаны аналитиками.

> Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Вы можете управлять инцидентами как объектами, используя следующие свойства инцидента:

- **Статус инцидента.**

  Статус инцидента показывает текущее состояние инцидента в его жизненном цикле. Вы можете изменить статус по своему усмотрению.

  Поддерживаются две модели статусов инцидентов. Подробности см. в разделе: Изменение статуса инцидента.

- **Уровень важности инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Уровень важности инцидента показывает, какое влияние этот инцидент может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень важности инцидента соответствует наивысшему уровню важности связанных алертов и не может быть изменен вручную.

- **Приоритет инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

- **Исполнитель инцидента.**

  Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

У каждого инцидента есть *свойства инцидента*, которые предоставляют всю информацию, связанную с инцидентом. Вы можете использовать эту информацию для расследования инцидента или объединения инцидентов.

Для каждого инцидента вы можете создавать дочерние инциденты. Дочерние инциденты позволяют вам исследовать инциденты и реагировать на них в разных тенантах. Вы также можете создать дочерний инцидент другого дочернего инцидента. Родительский инцидент может иметь не более 200 дочерних инцидентов.

Модель данных инцидента

Структура инцидента представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Alerts`).

Инцидент

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор инцидента (в формате UUID).
`ID`	Целое число	Да	Короткий внутренний идентификатор инцидента.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан инцидент (в формате UUID).
`IncidentType`	Объект `IncidentType`	Да	Тип инцидента.
`Имя`	Строка	Да	Название инцидента.
`WorkflowName`	Строка	Да	Имя рабочего процесса инцидента.
`WorkflowUUID`	Строка	Да	Уникальный идентификатор рабочего процесса инцидента в формате UUID.
`Описание`	Строка	Нет	Описание инцидента.
`CreatedAt`	Строка	Да	Дата и время создания инцидента (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения инцидента (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса инцидента (в формате RFC 3339).
`Severity`	Строка	Нет	Важность инцидента. Возможные значения: • `critical` • `high` • `medium` • `low`

`Приоритет`	Строка	Да	Приоритет инцидента. Возможные значения: • `critical` • `high` • `medium` • `low`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен инцидент.
`FirstEventTime`	Строка	Нет	Дата и время первого события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`LastEventTime`	Строка	Нет	Дата и время последнего события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`Состояние`	Строка	Да	Статус инцидента. Возможные значения: • `open` • `inProgress` • `hold` • `closed`
`StatusUUID`	Строка	Да	Идентификатор статуса инцидента (в формате UUID).
`StatusResolution`	Строка	Нет	Решение статуса инцидента. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`
`DetectSources`	Массив строк	Нет	Компоненты, которые обнаруживают и генерируют инцидент.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Alerts`	Массив объектов `Alert`	Нет	Алерты, включенные в инцидент.
`AdditionalData`	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
`ExternalRef`	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
`SignOfCreation`	Строка	Да	Способ создания инцидента.
`IsCII`	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
`Attachments`	Массив объектов `UnkeyedAttachment`	Нет	Вложения, связанные с инцидентом.

IncidentType

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор типа инцидента (в формате UUID).
`Имя`	Строка	Да	Имя типа инцидента.
`Описание`	Строка	Да	Описание типа инцидента.

Исполнитель

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор учетной записи оператора, которому назначен инцидент.
`Имя`	Строка	Да	Имя оператора, которому назначен инцидент.

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Имя`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Состояние`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Описание`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Создание инцидентов

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. В этой статье описано, как создавать инциденты вручную.

Чтобы иметь возможность создавать инциденты, у вас должны быть права на чтение и изменение алертов и инцидентов.

Если инцидент создается вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Вы можете создавать инциденты с помощью таблицы инцидентов или таблицы алертов.

Создание инцидентов с помощью таблицы инцидентов

Чтобы создать инцидент:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. Нажмите на кнопку **Создать инцидент**.

2. На шаге **Общие параметры** укажите следующие параметры:

   - Название инцидента.

   - **Тенант**

     Тенант, с которым связан инцидент. Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту. Вы не сможете изменить тенант инцидента позже.

   - **Исполнитель**

     Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

   - **Приоритет**

     Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

     Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

   - **Описание**

     В этом поле вы можете написать описание инцидента. Например, вы можете описать проблему или предоставить результаты расследования связанных алертов. Описание будет добавлено в раздел **Описание** в сведениях об инциденте.

     Поле не является обязательным.

3. Нажмите на кнопку **OK**.

   Инцидент создан.

Создание инцидентов с помощью таблицы алертов

Вы создаете инцидент, выбирая алерты для связи с новым инцидентом. См. как связать алерты с инцидентами.

Создание дочерних инцидентов

Дочерние инциденты позволяют вам отслеживать ход расследования инцидентов и реагировать на инциденты в разных тенантах. Вы также можете создать дочерний инцидент другого дочернего инцидента. Родительский инцидент может иметь до 200 дочерних инцидентов.

У вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Взаимодействие с дочерними инцидентами.

Создать дочерний инцидент:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно **Детали инцидента**.
3. В разделе **Дочерние инциденты** нажмите на кнопку **Создать**.

   Откроется окно **Создать дочерний инцидент**.
4. При необходимости в поле **Название** измените название дочернего инцидента.

   По умолчанию название дочернего инцидента включает тег [Child] и название родительского инцидента.
5. В раскрывающемся списке **Тенант** выберите тенант, которому будут назначены дочерние инциденты.
6. В раскрывающемся списке **Аналитик** начните вводить имя аналитика, а затем выберите его имя из списка.

   Вы также можете выбрать вариант **Не назначен**.
7. При необходимости раскрывающемся списке **Приоритет** измените приоритет инцидента.

   По умолчанию дочерний инцидент наследует приоритет от родительского инцидента.
8. При необходимости в поле **Описание** укажите описание дочернего инцидента.
9. Если вы хотите скопировать всю информацию из родительского инцидента, установите флажок **Копировать информацию из родительского инцидента**.

   Если этот флажок установлен, все данные, включая наблюдаемые объекты, активы и связанные алерты, будут скопированы из родительского инцидента. Скопированные алерты будут назначены тенанту дочернего инцидента.

Если этот флажок снят, дочерний инцидент не будет содержать информацию об активах, наблюдаемых и связанных алертах родительского инцидента.

10. Нажмите на кнопку **Создать**.

Дочерний инцидент создается и связывается с родительским инцидентом. Дочерний инцидент находится в разделе **Дочерние инциденты** окна **Детали инцидента**.

Если родительский инцидент имеет такой тип, которого нет у тенанта назначенному дочернему инциденту, то дочернему инциденту назначается тип инцидента по умолчанию и рабочий процесс инцидента по умолчанию. При необходимости вы можете изменить тип инцидента.

Просмотр таблицы инцидентов

Таблица инцидентов с обзором всех созданных инцидентов отображается в разделе **Мониторинг** → **Инциденты**. По умолчанию в таблице отображаются инциденты, относящиеся ко всем тенантам, к которым у вас есть права доступа. При необходимости таблицу инцидентов можно настроить.

Чтобы настроить таблицу инцидентов, выполните одно из следующих действий:

- Примените фильтр для тенантов:

  a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

  Откроется список тенантов.

  b. Установите флажки рядом с требуемыми тенантами.

- Отфильтруйте данные таблицы алертов:

  a. Нажмите на значок фильтра ( ).

  b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.

- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица инцидентов будет настроена, и в таблице отобразятся требуемые данные.

В таблице инцидентов есть следующие столбцы:

- **Создан**. Дата и время создания инцидента.
- **Продолжительность угрозы**. Время между самыми ранними и самыми последними событиями среди всех алертов, связанных с инцидентом.
- **Время обновления**. Дата и время последнего изменения в истории инцидента.
- **ID инцидента**. Уникальный идентификатор инцидента.
- **Статус**. Текущий статус инцидента.

- **Время на рассмотрение**. Срок рассмотрения инцидента в днях, часах и минутах.
- **Время, использованное на ответ**. Срок первоначального реагирования на инцидент в днях, часах и минутах.
- **Время на разрешение**. Срок разрешения инцидента в днях, часах и минутах.
- **Статус изменен**. Дата и время изменения статуса инцидента.
- **Важность.** Уровень важности инцидента.
- **Приоритет**. Приоритет инцидента.
- **Связан с алертами**. Сколько алертов включено в инцидент.
- **Название**. Название инцидента.
- **Правила**. Правила, которые сработали для создания инцидента.
- **Затронутые активы**. Устройства и пользователи, затронутые инцидентом. Если количество активов, затронутых инцидентом или вовлеченных в него, больше или равно трем, отображается количество затронутых устройств.
- **Тенант**. Имя тенанта, у которого был обнаружен инцидент.
- **Внешняя ссылка**. Номер инцидента во внешней системе.
- **Исполнитель**. Текущий исполнитель инцидента.
- **Есть родительский инцидент**. Наличие у инцидента родительского инцидента. Если отображается значение **Да**, инцидент является дочерним инцидентом.
- **Статус дочерних инцидентов**. Результирующий статус дочерних инцидентов первого уровня. Возможные значения: **Закрыто**, **В обработке**, **Дочерних инцидентов нет**.
- **Метод создания**. Как был создан инцидент, вручную или автоматически.
- **Наблюдаемые объекты**. Количество обнаруженных артефактов, например IP-адреса или MD5-хеши файлов. Если количество наблюдаемых объектов — три или больше, отображается количество наблюдаемых объектов.

Если требуется, можно экспортировать информацию обо всех инцидентах, которые отображаются в таблице инцидентов, в файл JSON.

Просмотр сведений об инциденте

Сведения об инциденте – это страница в интерфейсе, которая содержит всю информацию, относящуюся к инциденту, включая свойства инцидента.

Чтобы просмотреть сведения об инциденте:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.

При необходимости можно обновить информацию в деталях инцидента, нажав на кнопку обновления (🔄) рядом с названием инцидента.

Панель инструментов в верхней части информации об инциденте позволяет выполнять следующие действия:

- Изменить значения полей **Имя**, **Описание** и **Внешняя ссылка**.
- Просмотреть инцидент на графе расследования
- Изменить статус инцидента
- Изменить приоритет инцидента
- Назначить инцидент аналитику
- Выбрать плейбук
- Связать алерты с инцидентом
- Объединить инцидент с другими инцидентами

Сведения об инциденте содержат следующие разделы:

- **Сводная информация**

  Этот раздел содержит следующие свойства инцидента:

  - **Тип**. Тип инцидента.
  - **Аналитик**. Текущий исполнитель инцидента.
  - **Метод создания**. Как был создан инцидент, вручную или автоматически.
  - **Название**. Имя, указанное при создании инцидента. Вы можете нажать на кнопку **Изменить**, чтобы изменить название инцидента.
  - **Тенант**. Имя тенанта, у которого был обнаружен инцидент.
  - **Активы**. Количество пользователей и устройств, которые были затронуты инцидентом.
  - **Зарегистрировано**. Дата и время создания инцидента.
  - **Время обновления**. Дата и время последнего изменения в истории инцидента.
  - **Первое событие**. Дата и время первого события, связанного с инцидентом. Это самое раннее событие в разделе Детали алерта среди всех алертов, связанных с инцидентом.

- **Последнее событие.** Дата и время последнего события, связанного с инцидентом. Это последнее событие в разделе Детали алерта среди всех алертов, связанных с инцидентом.

- **Описание.** Описание инцидента. Вы можете нажать на кнопку **Изменить**, чтобы добавить описание.

- **Внешняя ссылка.** Ссылка на объект во внешней системе. Вы можете нажать на кнопку **Изменить**, чтобы указать внешнюю ссылку.

- **Приоритет**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критический**. Приоритет инцидентов определяет порядок, в котором инциденты могут расследоваться. Инциденты с приоритетом **Критический** являются наиболее важными и могут быть расследованы в первую очередь. Вы можете изменить приоритет, нажав на текущее значение приоритета.

- **Важность**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критический**. Уровень важности инцидента показывает, какое влияние этот инцидент может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского".

- **Время на рассмотрение** – срок рассмотрения инцидента в днях, часах и минутах.

- **Время на ответ** – срок первоначального реагирования на инцидент в днях, часах и минутах.

- **Время на разрешение** – срок разрешения инцидента в днях, часах и минутах.

- **Правила корреляции**. Правила, которые сработали для регистрации связанных алертов. Вы можете нажать на значок с многоточием рядом с названием правила, чтобы открыть контекстное меню. Используйте это меню, чтобы узнать больше о правиле, найти алерты или инциденты, которые были зарегистрированы этим же правилом, или найти события, инициировавшие правило, в разделе **Поиск угроз** за период между первым и последним событием инцидента. В заголовке раздела **Поиск угроз** отображаются идентификатор и имя инцидента, из которого был выполнен переход.

  Когда в меню вы нажимаете на раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается в той же вкладке. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- **IOA-правила**. IOA-правила, сработавшие для обнаружения угрозы и создания соответствующего алерта. Вы можете открыть контекстное меню, нажав на имя IOA-правила. В контекстном меню можно проводить следующие действия:

  - Просмотреть подробную информацию о конкретном IOA-правиле, нажав на кнопку **Открыть свойства**.

  - Просмотреть связанные события, нажав на кнопку **Перейти в Поиск угроз**.

    Выполняется перенаправление в раздел **Поиск угроз**, в котором отображаются только события, отслеживаемые данным правилом IOA. По умолчанию события отображаются за 24 часа. В заголовке раздела отображаются идентификатор и имя инцидента, из которого был выполнен переход.

  - Найти похожие инциденты.

  - Чтобы просмотреть подробную информацию о IOA-правиле в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.

  - Скопировать имя IOA-правила.

- **Тактика MITRE**. Тактика или несколько тактик, зарегистрированных в алертах, связанных с инцидентом. Вы можете открыть контекстное меню, нажав на имя тактики MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о тактике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о тактике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название тактики MITRE.
- **Техника MITRE**. Техника или несколько техник, зарегистрированных в алертах, связанных с инцидентом. Вы можете открыть контекстное меню, нажав на имя техники MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о технике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о технике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название техники MITRE.
- **Дополнительные данные**. Дополнительная информация об инциденте. Вы можете изменить значение в этом поле только с помощью плейбука. Поле отображается, если вы добавили значение.

- **Подробная информация**

  В разделе **Подробнее** вы можете отслеживать события телеметрии, связанные с инцидентом.

  Чтобы просмотреть события, связанные с инцидентом, нажмите на кнопку **Поиск угроз**. В открывшейся таблице отобразятся события алерта, связанные с инцидентом. В заголовке раздела **Поиск угроз** отображаются идентификатор и имя инцидента, из которого был выполнен переход.

  Панель инструментов таблицы событий позволяет выполнить следующие действия:

  - **Скачать события**. Нажмите на эту кнопку, чтобы скачать информацию о связанных событиях из файла TSV.
  - **Удалить связь с инцидентом**. Вы можете выбрать событие или несколько событий в таблице и нажать на эту кнопку, чтобы удалить связь выбранных событий с алертом, связанным с инцидентом.

  Вы можете вернуться к деталям инцидента, нажав на кнопку **Исследование инцидента** или на кнопку Назад в вашем браузере.

- **Подобные инциденты**

  В разделе **Подобные инциденты** вы можете просмотреть список инцидентов, которые имеют те же затронутые артефакты, что и текущий инцидент. Затронутые артефакты включают как наблюдаемые объекты, так и затронутые устройства алертов, связанных с инцидентом. В списке есть инциденты во всех статусах.

  С помощью вы можете оценить степень сходства текущего инцидента и других инцидентов. Сходство рассчитывается следующим образом:

  Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном инциденте, "T" – общее количество артефактов в текущем инциденте.

Если сходство составляет 100%, в текущем инциденте нет ничего нового по сравнению с аналогичным инцидентом. Если сходство равно 0%, текущий инцидент и схожий инцидент полностью различаются. Инциденты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор инцидента открывается подробная информация об инциденте.

Настройка списка похожих инцидентов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте инциденты, выбрав период, за который были обновлены инциденты. По умолчанию список содержит инциденты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать инциденты в порядке возрастания или убывания.

- **Алерты**

  В разделе **Алерты** вы можете просмотреть список алертов, связанных с текущим инцидентом.

  Нажав на идентификатор алерта, вы можете открыть детали алерта. Вы также можете использовать кнопки панели инструментов, чтобы удалить связь алерта с инцидентом.

- **Активы**

  В окне **Активы** можно выполнить следующие действия:

  - Просмотреть устройства и пользователей, затронутые алертом или вовлеченные в него.
  - Выполните действия по реагированию. Для этого установите флажок рядом с активом, а затем в раскрывающемся списке **Выбрать действие по реагированию** выберите необходимое действие по реагированию.
  - Чтобы экспортировать информацию о затронутых активах в CSV-файл, нажмите на кнопку **Экспортировать в CSV**.
  - Подключитесь к активу с помощью удаленного терминала. Для этого нажмите на кнопку **Открыть удаленный терминал**.

Таблица активов содержит следующие столбцы:

- **Тип актива**

  Возможные значения: устройство или пользователь.

- **Имя актива**

- **Идентификатор актива**

- **Статус авторизации**

  Этот параметр применяется только к типу актива – устройство. Статус авторизации устройства определяется KICS for Networks. Вы можете изменить статус авторизации, применив соответствующее действие по реагированию к устройству.

- **Имеет признаки**

  Возможные значения: атакующий или атакуемый.

- **Сервер администрирования**

  Сервер администрирования, который управляет устройством.

- **Категории**

  Категории активов, в которые входит актив.

- **Отправлено в архив**

  Статус объекта в архиве. Возможные значения: Yes или No.

- **Count**

  Количество устройств и пользователей, затронутых инцидентом или участвующих в нем, у которых одинаковый идентификатор, тип и имя.

- **Группа администрирования**

  Группа администрирования, к которой принадлежит пользователь.

Нажав на имя пользователя или устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.

- Скопировать имя пользователя или имя устройства в буфер обмена.

- Выполнить поиск по имени пользователя или идентификатору устройства в других алертах.

- Выполнить поиск по имени пользователя или идентификатору устройства в других инцидентах.

- Выполнить поиск имени пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием инцидента.

  Если после нажатия на имя пользователя или название устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

Нажав на идентификатор пользователя или идентификатор устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.

- Скопировать идентификатор пользователя или идентификатор устройства в буфер обмена.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других инцидентах.
- Выполнить поиск идентификатора пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием инцидента.

  Если после нажатия на идентификатор пользователя или идентификатор устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- **Дочерние инциденты**

  В разделе **Дочерние инциденты** вы можете просмотреть список инцидентов, которые являются дочерними для просматриваемого вами инцидента.

- **Файлы**

  Раздел **Файлы** содержит файлы, полученные в результате действий по реагированию или добавленные вручную в этот инцидент. Вы можете загружать, скачивать или удалять файлы, связанные с инцидентом, или изменять описание файлов.

  Вы можете загружать файлы любого расширения. Допускаются дубликаты имен файлов. Максимальное количество файлов, которые вы можете прикрепить к инциденту, и максимальный общий размер файлов, вы можете указать в конфигурационном файле.

  Ограничения по умолчанию:

  - Количество файлов не может превышать 100 на один инцидент.
  - Общий размер файла не может превышать 25 МБ на один инцидент.

Чтобы загрузить файлы, нажмите на кнопку **Загрузить** и выберите один или несколько файлов. Если вы попытаетесь загрузить файлы, превышающие ограничения, появится панель **Загрузка файлов** с предупреждающим сообщением. В этой панели вы можете удалять файлы из очереди загрузки до тех пор, пока не исчезнет предупреждающее сообщение, и нажать на кнопку **Загрузить**, чтобы загрузить файлы. Если вы нажмете на кнопку **Загрузить**, проигнорировав предупреждающее сообщение, загрузка не будет выполнена, а в списке файлов появятся файлы, которые не удалось загрузить, со значком предупреждения рядом с именами файлов.

После нажатия на кнопку **Загрузить** панель закрывается и загруженный файл отображается в таблице файлов в сведениях об инциденте и в главном меню приложения в разделе **Файлы**. При загрузке большого файла или нескольких файлов вам нужно обновить таблицу, чтобы в ней отображались новые файлы. Если загрузка файла выполняется, в столбце **Имя или полный путь** отображается индикатор загрузки, а в столбце **Размер** отображается размер уже загруженного файла.

Нажмите на файл, чтобы открыть панель **Изменить файл**, на которой отображаются сведения о файле. В этой панели вы можете изменить описание файла.

Используйте флажки для выбора файла или нескольких файлов. Выберите один или несколько файлов и нажмите на кнопку **Скачать**, чтобы скачать архив файлов в формате ZIP. Архив защищен паролем *infected*. Выберите файл или несколько файлов и нажмите на кнопку **Удалить**, чтобы удалить выбранные файлы.

Для загрузки и удаления файлов и изменения описаний файлов требуется право **Запись** в функциональной области **Алерты и инциденты**. Для возможности скачивать файлы требуется право на **Чтение** в функциональной области **Алерты и инциденты**.

- **Наблюдаемые объекты**

  В разделе **Наблюдаемые объекты** вы можете:

  - Просмотреть наблюдаемые объекты, которые относятся к алертам, связанными с текущим инцидентом.
  - Экспортировать информацию о связанных наблюдаемых объектах в CSV-файл, нажав на кнопку **Экспортировать в CSV**.
  - Выполнить поиск в таблице наблюдаемых объектов по данным из столбца **Значение**.

    Для этого в строке поиска начните вводить данные искомого наблюдаемого объекта. При отсутствии совпадений со значениями наблюдаемых объектов из столбца **Значение** отображается пустая таблица.

  Наблюдаемые объекты могут включать:

  - MD5-хеш
  - URL
  - Имя домена
  - SHA256
  - UserName
  - HostName
  - IP-адрес;

Следующие частные IP-адреса не включены в наблюдаемые объекты, связанные с алертами в текущем инциденте:
От 10.0.0.0 до 10.255.255.255 с маской подсети 255.0.0.0 или /8.
От 172.16.0.0 до 172.31.255.255 с маской подсети 255.240.0.0 или /12.
От 192.168.0.0 до 192.168.255.255 с маской подсети 255.255.0.0 или /16.
От 100.64.0.0 до 100.127.255.255 с маской подсети 255.192.0.0 или /10.

Чтобы включить частные IP-адреса в наблюдаемые данные, выполните следующие команды на устройстве администратора:

```
k0s kubectl -n irp set env deploy/transformer -c transformer
OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
```

```
k0s kubectl -n irp set env deploy/incident -c incident
OSMP_FILTER_PRIVATE_IPS_DISABLED=true
```

Нажав на ссылку в столбце **Значение**, вы можете:

- Выполнить поиск наблюдаемого значения в разделе **Поиск угроз** за период между первым и последним событием инцидента.

  Если после перехода по ссылке в столбце **Значение** вы выбираете в меню раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается на той же вкладке. В заголовке раздела отображаются идентификатор и имя инцидента, из которого был выполнен переход.Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- Выполнить поиск по значению наблюдаемого объекта в других алертах.
- Выполнить поиск по значению наблюдаемого объекта в других инцидентах.
- Скопировать значение наблюдаемого объекта в буфер обмена.

Панель инструментов этого раздела содержит следующие кнопки:

- **Запросить статусы Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). В результате информация обновляется в столбце **Статус обновления**. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Обогатить данные Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию обо всех перечисленных наблюдаемых объектах из Kaspersky TIP. В результате информация обновляется в столбце **Обогащение**. Используйте ссылку в столбце **Обогащение**, чтобы открыть полученные сведения об обогащении наблюдаемого объекта. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Поместить на карантин**. Используйте эту кнопку, чтобы переместить устройство, на котором находится файл, на карантин. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- **Добавить правило запрета**. Используйте эту кнопку, чтобы добавить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Удалить правило запрета**. Используйте эту кнопку, чтобы удалить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Прервать процесс**. Используйте эту кнопку, чтобы прервать процессы, связанные с файлом. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- **История**

  В разделе **История журнала событий** вы можете отслеживать изменения, внесенные в инцидент как в объект:

  - Изменение статуса инцидента.
  - Изменение исполнителя инцидента.
  - Связь алерта с инцидентом.
  - Удаление связи алерта с инцидентом.
  - Создание дочернего инцидента.
  - Объединение инцидента с другими инцидентами.
  - Загрузка файла в инцидент.
  - Удаление файла из инцидента.

  В разделе **История реагирований** вы можете просмотреть действия по реагированию, выполненные вручную, а также действия, выполненные в рамках плейбука. Таблица содержит следующие столбцы:

  - **Время**. Время возникновения события.
  - **Запущено**. Имя пользователя, запустившего действие по реагированию.
  - **События**. Описание события.
  - **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
  - **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
  - **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
    - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
    - **Запущено** – действие по реагированию выполняется.
    - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
    - **Предупреждение** – действие по реагированию завершено с предупреждениями.
    - **Ошибка** – действие по реагированию завершено с ошибками.

- **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
- **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
- **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.

- **Плейбук**. Название плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

- **Журнал трудозатрат**

  В разделе **Журнал трудозатрат** вы можете просмотреть трудозатраты аналитиков на работу с инцидентами.

  Раздел позволяем управлять вашими трудозатратами. Вы не можете изменять или удалять трудозатраты, добавленные другими аналитиками.

  Нажав на ссылку в столбце **Данные**, вы можете просмотреть и изменить свои трудозатраты.

- **Комментарии**

  В разделе **Комментарии** вы можете оставлять комментарии, связанные с инцидентом. Например, вы можете написать комментарий о результатах расследования или при изменении свойств инцидента, таких как исполнитель или статус инцидента.

  Чтобы сохранить комментарий, нажмите на клавишу **`Enter`**. Чтобы начать новую строку, нажмите на клавиши **`Shift + Enter`**. Чтобы изменить или удалить свой комментарий, используйте кнопки в правом верхнем углу.

  Вы можете редактировать и удалять собственные комментарии только в течение определенного промежутка времени после того, как оставите их. По умолчанию задан период в 15 минут.

  Если вы хотите изменить этот промежуток, выполните следующую команду на хосте администратора:

  ```
  k0s kubectl -n irp set env deploy/comment -c comment
  OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
  ```

  где `N` – промежуток времени, а `x` – единица измерения: `h` (часы) или `m` (минуты).

  Комментарии других пользователей невозможно изменить или удалить. Для возможности оставлять комментарии требуется право на **Запись** в функциональной области **Алерты и инциденты**.

Назначение инцидентов аналитикам

Как объект, инцидент должен быть передан аналитику SOC или группе пользователей для проверки и возможного расследования. Вы можете автоматически назначать инциденты аналитикам в выбранной группе пользователей. Подробнее см. раздел Настройка автоматического назначения алертов и инцидентов.

Вы можете изменить исполнителя инцидента в любое время.

> Инциденты можно назначить только аналитикам или группе пользователей, имеющим право на чтение и изменение алертов и инцидентов.

Чтобы назначить инцидент или несколько инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. Установите флажки напротив инцидентов, которые требуется назначить.

   Вам нужно выбрать только инциденты, обнаруженные в одном тенанте. Иначе кнопки **Назначить мне** и **Назначить** будут неактивны.

   Также вы можете назначить инцидент аналитику или группе пользователей из деталей инцидента. Чтобы открыть детали инцидента, нажмите на ссылку с идентификатором инцидента.
3. Выполните одно из следующих действий:
   - Чтобы назначить инциденты себе, нажмите на кнопку **Назначить мне**.
   - Чтобы назначить инциденты другому аналитику или группе пользователей:
     a. Нажмите на кнопку **Назначить**.
     b. В открывшемся окне **Назначить** выберите пользователя или группу пользователей, которым нужно назначить инциденты.
     c. Начните вводить имя аналитика или группы пользователей, а затем выберите исполнителя из списка.
     d. Нажмите на кнопку **Назначить**.

   Если вы хотите отменить назначение инцидентов, выберите **Не назначен**.

Инциденты назначены.

Также назначить аналитика для решения инцидента можно с помощью плейбуков.

Изменение статуса инцидента

Как объект, инцидент имеет статус, который показывает текущее состояние инцидента в его жизненном цикле.

Вы можете изменять статус для своих инцидентов или инцидентов других аналитиков, только если у вас есть право доступа для чтения и изменения алертов и инцидентов.

При изменении статуса инцидент и все неназначенные связанные алерты автоматически назначаются вам.

Если статус инцидента изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Инцидент может иметь один из следующих статусов:

- **Новый.**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *В обработке*, инцидент назначается вам автоматически. Когда вы меняете статус *Новый* на *Закрыт* и у инцидента нет исполнителя, он автоматически назначается вам.

- **В обработке.**

  This status means that an analyst started working on the incident or resumed the work by changing the *On hold* status. You can change the *In progress* status to any other status.

- **Отложен.**

  Этот статус означает, что аналитик приостановил работу над инцидентом. Обычно вы меняете статус *Отложен* на *В обработке*, когда работа возобновляется, но также можно изменить статус *Отложен* на другие статусы.

- **Закрыт**

  Вы закрываете инциденты, когда не требуется никакой дополнительной работы над инцидентом. Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыто* и наследуют решение инцидента. Если у инцидента нет исполнителя, закрытый инцидент автоматически назначается вам. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый инцидент в работу, измените его статус следующим образом: *Закрыт* → *Новый* → *В обработке*.

Чтобы изменить статус одного или нескольких инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить статус.
   - Перейдите по ссылке с идентификатором инцидента, статус которого вы хотите изменить.

     Откроется окно **Детали инцидента**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.

   Если выбран статус *Закрыто*, необходимо выбрать решение.

   Если для инцидента была нарушена хотя бы одна метрика SLA, при закрытии инцидента отображается поле **Причины нарушения SLA**. В этом поле нужно указать причину нарушения SLA.

   > Если при изменении статуса *Закрыто* в рабочем процессе инцидента был установлен флажок **Разрешить закрывать только этот инцидент только пользователям с определенными разрешениями**, для закрытия инцидента необходима роль EDR Главный администратор или Подтверждающий.

   > Если вы измените статус инцидента на *Закрыт* и этот инцидент содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.
5. Нажмите на кнопку **Сохранить**.

   Статусы выбранных инцидентов будут изменены.

Статус инцидента также можно изменить с помощью плейбуков.

Изменение приоритета инцидента

Как объект, инцидент имеет приоритет, который определяет порядок, в котором инцидент должен расследоваться аналитиками. Вы можете изменить приоритет инцидента вручную.

> Если у вас есть право доступа на чтение и изменение алертов и инцидентов, вы можете изменять приоритеты инцидентов для своих инцидентов или инцидентов других аналитиков.

Инцидент может иметь один из следующих приоритетов:

- **Низкий**.
- **Средний** (значение по умолчанию).

- **Высокий**.
- **Критический**.

Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. **Низкий** приоритет обычно означает, что инцидент помещен в очередь. Вы можете определить свои собственные критерии того, какой приоритет должен быть установлен для какого инцидента.

Чтобы изменить приоритет инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить приоритет.
   - Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте, приоритет которого вы хотите изменить.
3. Нажмите на кнопку **Изменить приоритет**.
4. В окне **Изменить приоритет** выберите приоритет, который нужно установить.
5. Нажмите на кнопку **Сохранить**.

   Приоритеты выбранных инцидентов будут изменены.

Также изменить приоритет инцидента можно с помощью плейбуков.

Для инцидента в статусе **Новый** (как только что созданного, так и переведенного в этот статус из любого другого):

- Вы можете редактировать приоритет, однако он автоматически пересчитывается при добавлении или удалении алерта из этого инцидента.

  Приоритет заполняется значением **Уровень важности инцидента**.
- Если вы вручную меняете приоритет инцидента, к которому не привязано ни одного алерта (инцидент создан без алертов либо все алерты удалены из инцидента), то **Уровень важности инцидента** заполняется значением приоритета.
- При пересчете приоритета SLA инцидента также пересчитывается автоматически.

Объединение инцидентов

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

Когда вы объединяете инциденты, вам нужно выбрать среди них целевой инцидент. После объединения инцидента проблему необходимо исследовать в рамках целевого инцидента. Целевой инцидент должен иметь статус, отличный от статуса *Закрытый*. Остальные инциденты объединяются в целевой и после объединения получают статус *Закрытый* и решение **Объединено**.

Все алерты, связанные с объединенными инцидентами, автоматически связываются с целевым инцидентом. Так как у инцидента не может быть более 1000 связанных алертов, приложение считает алерты, связанные с инцидентами, которые вы хотите объединить. Если общее количество связанных алертов превышает 1000, выбранные инциденты не могут быть объединены. При выборе целевого инцидента, отображается общее количество алертов после слияния.

Вы не можете объединять дочерние инциденты или инциденты, у которых есть дочерние инциденты.

Чтобы объединить инциденты из таблицы инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. Установите флажки рядом с инцидентами, которые требуется объединить в целевой инцидент. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить в инциденте**.
4. Откроется мастер **Объединить инциденты**.
5. Выберите целевой инцидент.
6. Нажмите на кнопку **Объединить**.

Инциденты объединены.

Чтобы объединить инциденты с использованием сведений об инциденте:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте. Этот инцидент будет объединен с целевым инцидентом. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить в инциденте**.

   Откроется мастер **Объединить инциденты**.
4. Выберите целевой инцидент.
5. Нажмите на кнопку **Объединить**.

Инциденты объединены.

Экспорт инцидентов в файл

Вы можете экспортировать инциденты в файл PDF или JSON.

Чтобы экспортировать инцидент в файл PDF:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**, чтобы открыть таблицу инцидентов.
2. Нажмите на идентификатор инцидента, который вы хотите экспортировать.

3. Нажмите на кнопку **Экспорт в PDF** в окне сведений инцидента.

   Откроется окно **Печать**.

4. В окне **Печать** разверните список **принтеров** и выберите **Сохранить как PDF**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить инцидент в виде PDF-файла.

   Если отсортировать таблицу инцидентов по полям **Тип** или **Название**, экспортированный PDF-файл также будет использовать эту сортировку.

Чтобы экспортировать все инциденты в файл JSON:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**, чтобы открыть таблицу инцидентов.

2. Нажмите на кнопку **Экспорт** в панели над таблицей событий.

3. Укажите имя файла и выберите папку, в которую нужно экспортировать инциденты.

4. Нажмите **Сохранить**, чтобы сохранить все инциденты в виде файла JSON.

Создание инцидентов Managed Detection and Response из EDR-инцидентов

Инцидент Managed Detection and Response можно создать из инцидента EDR, если в OSMP включена интеграция с Managed Detection and Response, а алерты инцидента соответствуют следующим условиям:

- Источником обнаружения является конечная точка.
- Выбранный инцидент имеет хотя бы один алерт, связанный с активом.
- Технология обнаружения может быть любой из следующих:
  - IOA-правила
  - IOC
  - YARA
  - SB (Sandbox)
  - AM (Anti-Malware Engine)

Порядок включения Managed Detection and Response в OSMP описан в статье Интеграция с приложениями и решениями "Лаборатории Касперского".

Чтобы экспортировать инцидент в Managed Detection and Response:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.

2. В таблице инцидентов нажмите на идентификатор требуемого инцидента. Откроется окно со сведениями об инциденте.

3. Нажмите на значок с тремя точками на панели инструментов и выберите **Создать инцидент MDR**.

4. В панели **Создать инцидент MDR** укажите имя и описание инцидента и нажмите на кнопку **Создать**.

   Если инцидент создан успешно, отображается соответствующее сообщение. Теперь вы можете получить доступ к инциденту в Консоли MDR. Ссылка на инцидент доступна в разделе сводной информации инцидента EDR.

Правила сегментации

Правила сегментации позволяют автоматически разделять связанные алерты на разные инциденты в соответствии с условиями, которые указанными при создании правил.

Используйте правила сегментации для создания отдельных инцидентов на основе связанных алертов. Например, вы можете объединить несколько алертов с важной отличительной чертой в отдельный инцидент.

Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту.

Правила сегментации срабатывают в соответствии с указанным приоритетом. Чем выше находится правило в списке правил сегментации, тем выше его приоритет. Если вы хотите изменить приоритет правила сегментации, вам нужно перетащить правило, нажав на его имя.

Рекомендуется использовать правила сегментации вместе с правилами агрегации для определения более точных правил создания инцидентов.

Чтобы создать правило сегментации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила сегментации**.

   Откроется список правил сегментации.

2. Нажмите на кнопку **Создать**.

   Откроется окно **Создать правило сегментации**.

3. Укажите параметры сегментации правила.

   - **Статус**

     Включите или выключите правило. По умолчанию правило выключено.

   - **Правило**

     Укажите уникальное имя правила.

   - **Максимум алертов в инциденте**

     Максимальное количество алертов в одном инциденте. Значение должно укладываться в диапазон от 1 до 200, а также должно быть больше или равно значению **Минимум алертов в инциденте**. Значение по умолчанию – 200. Если количество алертов превышает указанное значение, создается другой инцидент.

   - **Минимум алертов в инциденте**

     Минимальное количество алертов в одном инциденте. Минимальное значение и значение по умолчанию – 1. Значение должно быть меньше или равно значению **Максимум алертов в инциденте**. Если количество алертов не достигает указанного значения, инцидент не создается.

- **Интервал поиска**

  Период, из которого следует выбирать алерты и инциденты. Значение можно указать в днях или часах. По умолчанию указано значение 30 дней.

- **Описание**

  Необязательно. Описание правила.

- **Группы**

  Выражение jq, определяющее массив идентификаторов строк, по которым назначаются алерты инцидентам.

  При необходимости вы можете скопировать выражение jq для раздела **Группы** из другого правила сегментации. Для этого нажмите на кнопку **Копировать из другого правила**.

  Пример: `if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then ["Brute force admin"] else ["Brute force not admin"] end`

- **Название инцидента**

  Выражение jq, определяющее шаблон наименований инцидентов, созданных в соответствии с этим правилом сегментации. По умолчанию указано следующее выражение: `"\(.Rules[]?.Name), \(.SourceCreatedAt)"`

  Выражение jq для раздела **Название инцидента** можно скопировать из другого правила сегментации. Для этого нажмите на кнопку **Копировать из другого правила**.

  Пример: `if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then "Brute force admin" else "Brute force not admin" end`

- **Триггер**

  Выражение jq, определяющее условие включения алертов в инцидент.

  При необходимости вы можете скопировать выражение jq для раздела **Триггер** из другого правила сегментации. Для этого нажмите на кнопку **Копировать из другого правила**.

  Пример: `any(.Rules[]?; .ID == "123")`

4. Нажмите на кнопку **Сохранить**.

Правило сегментации сохраняется и отображается в таблице правил сегментации. Параметры правила можно изменить, нажав на его название в таблице.

Вы можете использовать логический оператор `inSubnet` в выражениях jq, чтобы проверить, находится ли левый операнд (IP-адрес) в подсети правого операнда (подсеть).

Пример: `any(.Observables[]? | select(.Type == "ip") | .Value // empty; inSubnet("11.11.11.1/11"))`

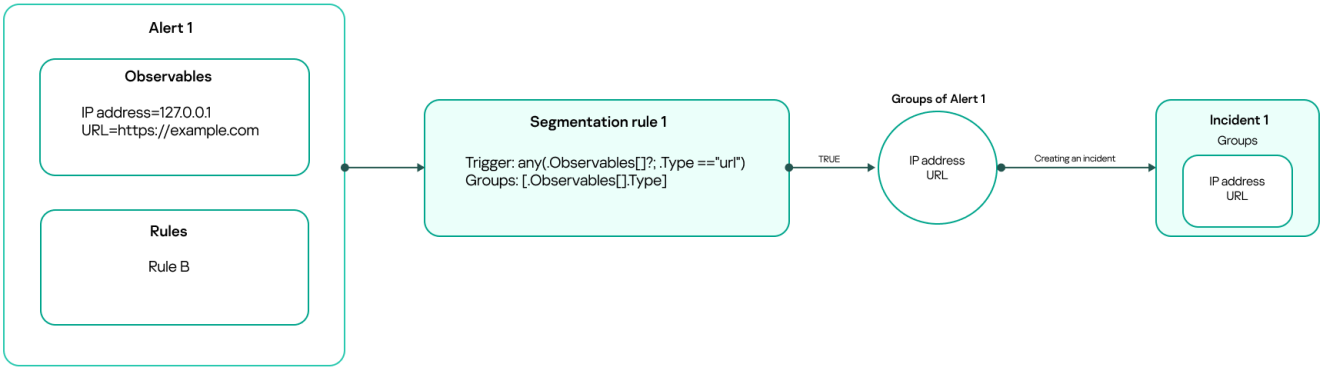
Доступны следующие предварительно заданные правила сегментации:

- Ссылки на существующий инцидент: одинаковый хеш файла MD5
- Ссылки на существующий инцидент: одинаковый актив хоста
- Ссылки на существующий инцидент: одинаковые правила IOA, IOC или YARA
- Создать инцидент: одинаковый хеш файла MD5

- Создать инцидент: одинаковый актив хоста
- Создать инцидент: одинаковые правила IOA, IOC или YARA

Предварительно заданные правила автоматически применяются к тенантам.

Создаваемые алерты проверяются по всем активным правилам сегментации в соответствии с их приоритетом. После срабатывания первого правила для алерта формируется массив строковых идентификаторов и начинается поиск инцидента, с которым должен быть связан алерт.

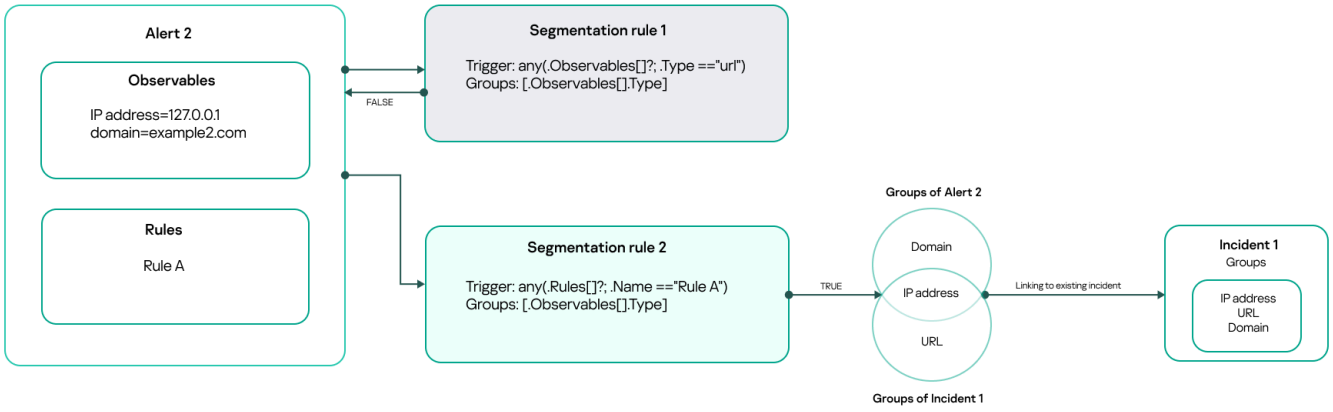


Создание инцидента после срабатывания первого правила сегментации

Правило срабатывает, если выражение jq, указанное в **разделе Триггер**, возвращает значение `true`.

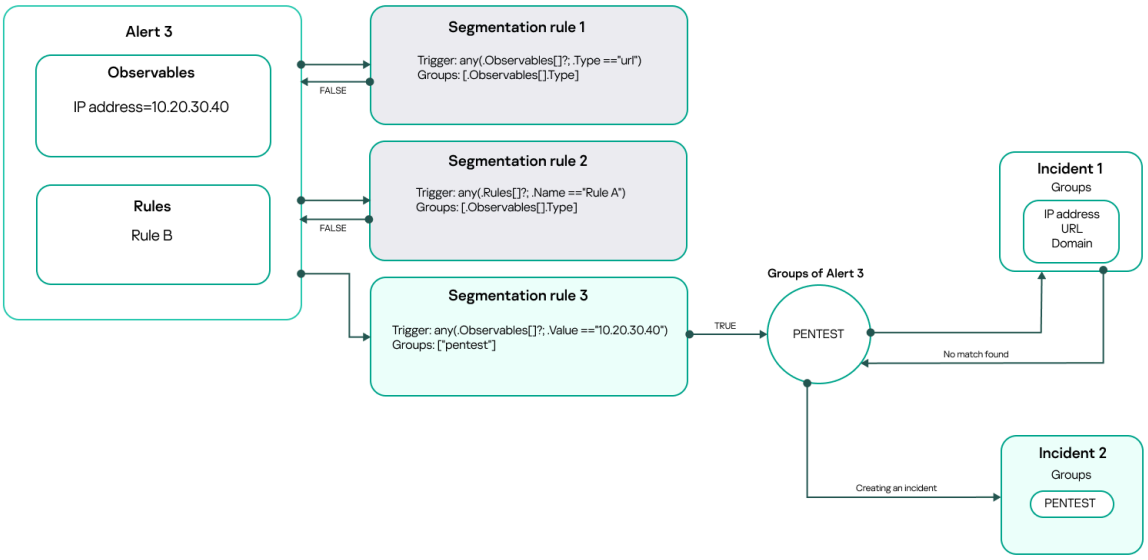
Алерты не могут быть связаны с инцидентами, созданными вручную.

У инцидента также есть массив строковых идентификаторов, который включает в себя массивы алертов, уже связанных с этим инцидентом. Если в массиве алерта, для которого сработало правило сегментации, есть хотя бы один элемент, совпадающий с любым из элементов в массиве инцидента, алерт связывается с этим инцидентом. В результате массив этого алерта добавляется в массив инцидента.



Привязка алерта к существующему инциденту после обнаружения совпадающих элементов

Если существует несколько инцидентов, удовлетворяющих условию, алерт связывается с инцидентом с наиболее поздним обновлением. Если в массивах не находится инцидентов с подходящими элементами, создается новый инцидент.



Создание инцидента после того, как не найдено ни одного подходящего элемента на основе первых двух правил сегментации

У новых инцидентов массив пуст. Массив строковых идентификаторов для нового инцидента берется из алерта после связывания алерта.

Правило сегментации. Пример

Настройте правила агрегации в разделе Правила агрегации. Пример раздела в этой статье.

В таблице ниже показано, как объединить все тестовые алерты на проникновение в один инцидент.

Правило сегментации

Атрибут	Значение
Триггер	.AggregationID == "Pentest"
Группы	["Pentest"]
Название инцидента	"Pentest incident"

Правила агрегации и сегментации. Пример

В таблица ниже описано, как объединить алерты, имеющие одинаковый идентификатор правила, в двух инцидентах на основе префикса имени пользователя.

Правило агрегации

Атрибут	Значение	Описание
Триггер	any(.Rules[]?; .ID == "123")	Поиск алертов с идентификатором правила "123".

Идентификатор правила агрегации	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "rule123_DestinationUserName_adm" else "rule123_DestinationUserName_not_adm" end	Поиск имен пользователей с префиксом "adm_".
Название алерта	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Rule123 admin" else "Rule123 not admin" end	Устанавливает название алерта в зависимости от префикса имени пользователя.

Правило сегментации

Атрибут	Значение
Триггер	.AggregationID | startswith("rule123_DestinationUserName")
Группы	[.AggregationID]
Название инцидента	.Name

Копирование правил сегментации в другой тенант

Вы можете скопировать существующее правило сегментации другому тенанту.

Если иерархия экземпляров OSMP построена, вы можете копировать правила только внутри экземпляра.

Чтобы скопировать правила сегментации:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила сегментации**.

   Откроется таблица правил сегментации.

2. Выберите правила сегментации, которые вы хотите скопировать, и нажмите на кнопку **Копировать в тенант**.

3. Выберите один или несколько целевых тенантов и нажмите на кнопку **Копировать**.

4. Если целевой тенант содержит правило сегментации с таким же именем, откроется окно **Перезаписать или переименовать правила сегментации?**.

   Нажмите на кнопку **Перезаписать**, чтобы удалить ранее созданное правило для целевого тенанта и заменить его правилом, которое вы хотите скопировать.

   Нажмите на кнопку **Копировать и переименовать**, чтобы сохранить ранее созданное правило и скопировать указанное правило с добавлением `(copy)` к его заголовку.

   Если вы копируете унаследованное правило, а у целевого тенанта уже есть правило с таким же именем, оно не будет перезаписано. Вам нужно изменить имя правила, которое вы копируете. Также унаследованные правила копируются со своим статусом, но без области действия.

   При нажатии на кнопку закрытия (×) окно закрывается, а правила сегментации, имена которых совпадают с именам в целевых тенантах, не копируются. Если на шаге 2 вы также выбрали правила сегментации, которых нет в целевых тенантах, такие правила копируются.

Правила сегментации копируются другому тенанту или тенантам.

Управление Service Level Agreement (SLA)

Kaspersky EDR Expert позволяет настраивать Service Level Agreement (SLA), которые определяют сроки обработки инцидентов.

Вы можете определить SLA для комбинации рабочего процесса инцидента и приоритета.

Таблица **Инциденты** и сведения об инцидентах показывают оставшееся время для SLA.

Вы можете настроить шаблон уведомления по электронной почте с типами **Истекает SLA инцидента** и **SLA инцидента изменено**.

Перезапуск расчета показателей SLA при возврате исходного статуса инцидента

Показатели SLA не рассчитываются для инцидента, когда инцидент считается обработанным. По умолчанию возврат статуса инцидента к исходному статусу приводит к перезапуску показателей SLA.

Чтобы предотвратить перезапуск показателей SLA при возврате исходного статуса инцидента:

1. Убедитесь, что на устройстве администратора установлена утилита kubectl.
2. Выполните следующую команду:

   ```
   kubectl -n irp set env deploy/incident
   OSMP_INCIDENT_SLA_DISABLE_RESTART_CALCULATION_ON_START_TRIGGER=true
   ```

3. Перезапустите службу инцидента.

Создание Service Level Agreement (SLA)

Для создания записей SLA у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, администратор SOC.

Чтобы создать SLA:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Откройте вкладку **Параметры** и нажмите **Управление инцидентами**.
4. Выберите вкладку **SLA** и нажмите на кнопку **Создать**.

5. В открывшейся панели **Создать SLA** настройте следующие параметры:

   - **Название SLA** – отображаемое имя SLA.
   - **Приоритет** – приоритет инцидента, к которому применяется SLA.
   - **Рабочий процесс** – рабочий процесс инцидента, к которому применяется SLA.

     Вы можете назначить только одно SLA для комбинации **Рабочий процесс** и **Приоритет**. Вы не можете выбрать рабочие процессы инцидентов, которые используются в других SLA с таким же приоритетом.
   - **Время на рассмотрение** – срок рассмотрения инцидента в днях, часах и минутах. Инцидент считается принятым, когда его статус меняется с одного на другой.

     Чтобы определить этот переход, выберите значения **Из статуса** и **В статус**.
   - **Время на ответ** – срок первоначального реагирования на инцидент в днях, часах и минутах.

     Выберите условие остановки:

     - Если вы хотите, чтобы инцидент считался обработанным после применения действия по реагированию, выберите **При первом действии по реагированию**. После этого выберите одно или несколько значений в поле **Из статуса**.
     - Если вы хотите, чтобы инцидент считался обработанным после того, как его статус изменился на другой, выберите **При смене статуса на**. После этого выберите одно или несколько значений в полях **Из статуса** и **В статус**.
   - **Время на разрешение** – срок разрешения инцидента в днях, часах и минутах. Инцидент считается разрешенным, когда его статус меняется с одного на другой.

     Чтобы определить этот переход, выберите значения **Из статуса** и **В статус**.

6. Нажмите на кнопку **Создать**.

   Созданное SLA отобразится в таблице.

Удаление Service Level Agreement (SLA)

Для удаления записей SLA у вас должна быть одна из следующих EDR-ролей: Главный администратор, администратор тенанта, администратор SOC.

Чтобы удалить SLA:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Откройте вкладку **Параметры** и нажмите **Управление инцидентами**.

4. Выберите вкладку **Удалить**.

5. Установите флажок напротив SLA, которое нужно удалить.

6. Нажмите на кнопку **Удалить**.

7. В окне подтверждения нажмите на кнопку **Удалить**.

При удалении SLA сроки для инцидентов с указанием значений **Тип инцидента** и **Приоритет** больше не рассчитываются.

Работа с типами инцидентов

Kaspersky EDR Expert позволяет управлять инцидентами и настраивать процесс обработки инцидентов с помощью типов инцидентов.

Тип инцидента – это набор атрибутов, для которых вы можете настроить различные процессы, например, назначить рабочий процесс для типа инцидента, настроить триггер или алгоритм плейбука.

Вы можете создать тип инцидента или использовать предустановленные типы инцидентов, которые вы можете настроить.

Типы инцидентов могут быть активными или неактивными. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.

Тип инцидента, отмеченный как тип по умолчанию, автоматически назначается всем новым инцидентам. Вы не можете переключить тип инцидента по умолчанию в неактивный.

Тип инцидента **Общий** установлен как значение по умолчанию. Вы можете изменить этот параметр.

В тенанте вы можете создать только один тип инцидента по умолчанию.

Просмотр таблицы типов инцидентов

Чтобы просмотреть таблицу типов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.

4. Если вы хотите настроить таблицу типов инцидентов, выполните любое из следующих действий:

   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

   - Чтобы скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

В таблице типов инцидентов содержится следующая информация:

- **Название**. Название пользовательских или предустановленных типов инцидентов.

  В таблице содержатся следующие предустановленные типы инцидентов:

  - Общие.

    > По умолчанию этот тип имеет значение **Да** в столбце **По умолчанию**.

  - Получение информации.
  - Компрометация.
  - Несанкционированный доступ.
  - Атака вредоносного ПО.
  - Фишинг.
  - Доступность.
  - Угроза изнутри.
  - Нарушение безопасности данных.
  - Ошибка конфигурации.
  - Атака через цепочку поставок.
  - Атака веб-приложения.
  - Использование уязвимостей.

- **Активный тип**. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.

- **По умолчанию**. При создании инцидента, ему автоматически присваивается тип по умолчанию. Возможные значения:

  - **True.**
  - **False.**

- **Рабочий процесс**. Рабочий процесс инцидента.

- **Тенант**. Имя тенанта, которому принадлежит тип инцидента.

- **Тип создания**. Способ создания типа инцидента. Возможные значения:

  - **Пользовательский**
  - **Предопределенный**

- **Идентификатор**. Уникальный идентификатор пользовательского или предустановленного типа инцидента. По умолчанию этот столбец скрыт.

- **Описание**. Описание типа инцидента. По умолчанию этот столбец скрыт.

При необходимости, вы можете создавать новые типы инцидентов, а также изменять и удалять предустановленные и пользовательские типы инцидентов.

Создание типов инцидентов

Чтобы создать тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Типы**.

4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать тип инцидента**.

5. Если вы хотите, чтобы новый тип инцидента был активным, включите переключатель **Активный тип**.

6. В поле **Название** введите название нового типа инцидента.

7. Если вы хотите, чтобы всем новым инцидентам по умолчанию назначался этот тип, установите флажок **Сделать по умолчанию**.

   > В тенанте может быть только один тип инцидентов по умолчанию. Это означает, что, если у тенанта уже есть тип инцидента по умолчанию, этот тип больше не будет типом по умолчанию после того, как вы установите этот флажок.

8. В поле **Рабочий процесс** выберите рабочий процесс инцидента.

9. При необходимости в поле **Описание** укажите описание типа инцидента или комментарий.

10. Нажмите на кнопку **Создать**.

    Новый тип инцидента отобразится в таблице типов инцидентов.

Изменение типов инцидентов

При необходимости вы можете изменять типы инцидентов.

Чтобы изменить тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.
4. Нажмите на имя типа инцидента, который требуется изменить.

   Откроется окно **Изменить тип инцидента**.
5. Внесите изменения и нажмите на кнопку **Сохранить**. Дополнительные сведения о свойствах типов инцидентов, которые вы можете изменить, см. в разделе Создание типов инцидентов.

Свойства типа инцидента изменены и сохранены.

Удаление типов инцидентов

Если вы хотите удалить тип инцидента, который используется в плейбуке, вам нужно удалить этот тип инцидента из триггера плейбука и/или алгоритма, чтобы избежать ошибок.

Удалить тип инцидента невозможно в следующих случаях:

- Тип инцидента установлен по умолчанию в тенанте, где был создан этот тип инцидента.

  При попытке удалить этот тип инцидента, вам будет предложено установить новый тип инцидента по умолчанию. В открывшемся окне вам нужно выбрать тип инцидента из списка.
- Тип инцидента установлен по умолчанию в дочернем тенанте.
- Текущий тенант или дочерний тенант содержит инцидент с типом, который вы хотите удалить.

  Прежде чем удалить такой тип, вам нужно назначить инциденту другой тип.
- Для типа инцидента определено правило Service Level Agreement (SLA).

Чтобы удалить тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.

4. Выполните одно из следующих действий:

   - Выберите тип инцидента, который вы хотите удалить и нажмите на кнопку **Удалить**.

   - Нажмите на название типа инцидента, который вы хотите удалить, затем в окне **Изменить тип инцидента**, нажмите на кнопку **Удалить**.

5. В диалоговом окне нажмите на кнопку **Удалить**.

   Тип инцидента будет удален.

Управление типами рабочих процессов

Kaspersky EDR Expert позволяет настраивать гибкий рабочий процесс инцидента. Kaspersky EDR Expert также отображает рабочий процесс в визуальном редакторе.

Процесс обработки инцидента представляет собой набор статусов и переходов, через которые проходит инцидент в течение его жизненного цикла. *Статус* является шагом в процессе обработки инцидента. *Переход* помогает инциденту переходить в различные статусы. Переход – это ссылка, которая позволяет настраивать переходы от одного статуса инцидента к другому и обратно. При необходимости, вы можете использовать переход как однонаправленную ссылку.

Вы можете создать рабочий процесс инцидента или использовать предустановленный рабочий процесс, который можно настроить.

Также можно назначить рабочий процесс типам инцидентов. Это поможет вам управлять жизненным циклом инцидента наиболее удобным образом.

Просмотр таблицы рабочих процессов инцидентов

Чтобы просмотреть таблицу рабочих процессов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.

   Чтобы скрыть или отобразить столбец, нажмите на значок параметров (⚙) и выберите нужный столбец.

   Отобразится таблица рабочих процессов инцидентов.

В таблице рабочих процессов инцидентов содержится следующая информация:

- **Название**. Название пользовательских или предустановленных рабочих процессов инцидентов.

- **Связанные типы**. Количество связанных типов инцидентов.

- **Имя тенанта**. Имя тенанта, которому принадлежит рабочий процесс инцидента.

- **Тип создания**. Способ создания рабочего процесса инцидента. Возможные значения:
  - **Пользовательский**.
  - **Предопределенный**.
- **Идентификатор рабочего процесса**. Уникальный идентификатор рабочего процесса инцидента. По умолчанию этот столбец скрыт.
- **Описание**. Описание рабочего процесса инцидента. По умолчанию, этот столбец скрыт.

Предустановленные рабочие процессы инцидентов

Kaspersky EDR Expert позволяет управлять инцидентами с помощью предустановленного рабочего процесса инцидента. В таблице рабочих процессов инцидентов, такой рабочий процесс называется **Стандартный**. В столбце **Тип создания** эти рабочие процессы отмечены как **Предопределенный**.

При необходимости, вы можете изменить предустановленный рабочий процесс.

В таблице ниже описаны статусы предустановленного рабочего процесса и причины, по которым инцидентам присваиваются эти статусы.

Состояние	Причины
Новый	• Инцидент создан (вручную или автоматически). • Статус инцидента был изменен на **Новый** с одного из следующих статусов: **В обработке**, **Отложен** или **Закрыт**.
В обработке	Пользователь вручную изменил статус инцидента с **Новый** или **Отложен** на **В обработке**.
Отложен	Пользователь вручную изменил статус инцидента с **В обработке** на **Отложен**.
Закрыт	• Пользователь закрыл инцидент. • Пользователь связал инцидент с другим похожим инцидентом, который еще не был закрыт.

Рабочий процесс по ГОСТ

Kaspersky EDR Expert предоставляет возможность использовать для управления инцидентами рабочий процесс, созданный на основании ГОСТ Р 59712-2022. По умолчанию, в таблице рабочих процессов он имеет название **ГОСТ** и является предустановленным.

При необходимости вы можете изменить рабочий процесс **ГОСТ** под свои нужды.

Рабочий процесс **ГОСТ** состоит из следующих статусов:

- **Новый**. Создание инцидента (ручное или автоматическое).
- **Анализ**. Изучение негативного воздействия на элементы информационной инфраструктуры.
- **Локализация**. Определение элементов информационной инфраструктуры, которые подверглись негативному воздействию.
- **Последствия**. Определение последствий негативного воздействия на элементы информационной инфраструктуры.

- **Ликвидация**. Ликвидация причины, а также последствий негативного воздействия на элементы информационной инфраструктуры.
- **Выполнен**. Последствия негативного воздействия устранены, причины выявлены.
- **Закрыт**. Проверка достаточности выполненных действий по ликвидация причин и последствий негативного воздействия на элементы информационной инфраструктуры.

Создание рабочих процессов инцидентов

Рабочий процесс инцидента позволяет управлять жизненным циклом инцидента.

Чтобы создать рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать рабочий процесс**.

   > По умолчанию каждый рабочий процесс инцидента содержит предустановленные статусы **Новый** и **Закрыт**. Вы не можете удалить или изменить эти статусы.
5. В поле **Название** введите название нового рабочего процесса.
6. При необходимости в поле **Описание** введите описание рабочего процесса или комментарий.
7. Чтобы добавить новые статусы, в разделе **Рабочий процесс** нажмите **Добавить статус**.
8. В открывшемся окне настройте следующие параметры:

   a. В поле **Название статуса** введите название нового статуса.

   b. В поле **Категория** выберите одну из следующих категорий статуса:

      - **Новый**
      - **В обработке**
      - **Решен**
      - **Закрыт**

      Категория определяет цвет значка статуса.

c. В поле **Входящий переход** выберите один или несколько входящих статусов.

Если вы хотите настроить переход от всех статусов к входящим статусам, выберите параметр **Разрешить всем статусам переходить на этот**.

d. В поле **Исходящий переход**, выберите один или несколько исходящих статусов.

Если вы хотите настроить переход от исходящих статусов ко всем статусам, выберите параметр **Разрешить этому статусу переходить на все статусы**

e. Нажмите на кнопку **Добавить**.

Визуализированный рабочий процесс отображается в окне **Создать рабочий процесс**

При необходимости повторите шаги 7 и 8, чтобы добавить новые статусы.

9. В окне **Создать рабочий процесс** нажмите на кнопку **Сохранить**.

Новый рабочий процесс инцидента отобразится в таблице.

Изменение рабочих процессов и статусов инцидентов

Вы можете изменить свойства рабочего процесса, а также статусы и переходы рабочего процесса.

Чтобы изменить рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.
5. Измените свойства рабочего процесса. Дополнительные сведения о свойствах рабочего процесса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

Свойства рабочего процесса изменены и сохранены.

Чтобы изменить статусы рабочего процесса инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.
5. Нажмите на название статуса, который требуется изменить.

   Откроется окно **Изменить статус**.

6. Измените параметры статуса и параметры перехода. Дополнительные сведения о параметрах статуса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

   При необходимости, вы можете удалить статус, нажав на кнопку **Удалить**.

   Вы не можете изменить название и категорию следующих предустановленных статусов: **Новый** и **Закрыт**. Вы также не можете удалить эти предустановленные статусы.

   Вы не можете удалить статус, если он назначен инциденту.

7. Нажмите на кнопку **Сохранить**.

Статусы рабочего процесса изменены и сохранены.

Удаление рабочих процессов инцидентов

Вы не можете удалить рабочий процесс инцидента, если есть связанные типы инцидентов, которые принадлежат родительскому или дочернему тенанту. В этом случае вам нужно назначить другой рабочий процесс связанным типам инцидентов, а затем попробовать снова удалить рабочий процесс инцидента.

Если вы хотите удалить рабочий процесс, который используется в плейбуке, перед удалением измените триггер и/или алгоритм плейбука, чтобы избежать ошибок.

Чтобы удалить рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. В списке рабочих процессов выберите рабочий процесс, который вы хотите удалить, и нажмите на кнопку **Удалить**.
5. В диалоговом окне нажмите на кнопку **Удалить**.

Рабочий процесс инцидента удален.

Управление трудозатратами инцидентов

Kaspersky EDR Expert позволяет отслеживать трудозатраты на работу с инцидентами. Это помогает рассчитывать время, затрачиваемое аналитиком на анализ инцидентов и реагирование на них, оценивать рабочую нагрузку на аналитика и эффективным образом распределять трудовые ресурсы.

Аналитики могут вручную вводить данные о своих трудозатратах по работе с инцидентом, включая затраченное время и категорию трудозатрат, если это необходимо.

Категории трудозатрат можно просматривать, добавлять, изменять или удалять через API. Чтобы управлять категориями трудозатрат, вам нужно иметь одну из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC.

Для управления трудозатратами инцидентов у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий.

Kaspersky EDR Expert также позволяет формировать и экспортировать отчеты о трудозатратах аналитиков или групп пользователей для дальнейшего анализа.

Добавление трудозатрат инцидентов

Вы можете добавить трудозатраты на работу с инцидентом в раздел **Журнал трудозатрат** подробных данных инцидента. Это помогает анализировать время, затрачиваемое аналитиками на обработку инцидентов, планировать свою рабочую нагрузку и рассчитывать затраты на заработную плату.

Чтобы добавить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Перейдите на вкладку **Журнал трудозатрат** и нажмите на кнопку **Добавить**.

   Откроется панель **Добавить трудозатраты**.
4. При необходимости в раскрывающемся списке **Категория** выберите категорию трудозатрат.
5. В полях **Часы** и **Минуты** укажите время, которое вы потратили на работу с инцидентом.

   Максимальное значение поля **Минуты** – 59.
6. Нажмите на кнопку **Добавить**.

Трудозатраты на работу с инцидентами будут добавлены.

Изменения трудозатрат инцидентов

Вы можете изменить ранее добавленные трудозатраты.

Невозможно изменять трудозатраты, добавленные другими аналитиками.

Чтобы изменить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Перейдите на вкладку **Журнал трудозатрат**.
4. В столбце **Дата** перейдите по ссылке с датой и временем трудозатрат, которые вы хотите изменить.

   Откроется панель **Изменить трудозатраты**.
5. Измените трудозатраты и нажмите на кнопку **Сохранить**.

Трудозатраты будут изменены и сохранены.

Удаление трудозатрат инцидентов

Вы можете удалить ранее добавленные трудозатраты.

Невозможно удалить трудозатраты, добавленные другими аналитиками.

Чтобы удалить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Перейдите на вкладку **Журнал трудозатрат**.
4. В списке трудозатрат установите флажки рядом с трудозатратами, которые вы хотите удалить и нажмите на кнопку **Удалить**.

Трудозатраты будут удалены.

Создание и экспорт отчетов об инцидентах

Вы можете формировать и экспортировать отчеты о трудозатратах аналитиков на работу с инцидентами и отчеты о соответствии инцидентов метрикам SLA. Отчеты сохраняются в формате CSV.

Чтобы сформировать отчет об инциденте, вам нужно:

- Иметь доступ к тенанту, к которому принадлежит инцидент.
- Иметь одну из следующих XDR-ролей: Главный администратор, Администратор SOC, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Аудитор.

Чтобы сформировать и экспортировать отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.

2. В панели инструментов нажмите на кнопку **Экспортировать** и в открывшемся меню выберите один из следующих вариантов:

   - **Отчет о трудозатратах** для экспорта трудозатрат аналитиков на работу с инцидентом.

   - **Отчет о метриках инцидента** для экспорта отчета о соответствии инцидентов показателям SLA.

3. В открывшейся панели укажите период, за который вы хотите отобразить данные в отчете. Для этого выберите дату и время в полях **От** и **По**.

   По умолчанию в поле **От** выбран первый день текущего месяца, а время установлено на 00:00. В поле **По** выбрана текущая дата и установлено время 23:59.

4. При необходимости укажите другие параметры в зависимости от типа отчета, который вы выбрали на шаге 3:

   - Если выбран **Отчет о трудозатратах**:

     - Выберите аналитиков или группы пользователей, чтобы в отчет были включены их трудозатраты на работу с инцидентами.

     - Включите переключатель **Включить идентификатор инцидента и сведения о категории трудозатрат**, если вы хотите, чтобы отчет о трудозатратах содержал эти сведения.

       По умолчанию переключатель выключен.

   - Если выбран **Отчет о метриках инцидента**:

     - Выберите приоритеты инцидентов, которые будут включены в отчет. Возможные значения: **Низкий**, **Средний**, **Высокий**, **Критический**.

     - Включите переключатель **Экспортировать только инциденты с нарушениями SLA**, если вы хотите включать в отчет только инциденты с нарушением SLA.

       Инцидент включается в отчет, если у него есть хотя бы одна запись SLA с истекшим сроком действия. Запись SLA истекла, если хотя бы одно из ее значений (**Время на рассмотрение**, **Время, использованное на ответ** или **Время на разрешение**) меньше 0.

5. Нажмите на кнопку **Экспортировать**.

Панель закроется, отчет будет создан и загружен на ваше устройство.

Настройка периода хранения алертов и инцидентов

Kaspersky EDR Expert позволяет вам уменьшать или увеличивать период хранения алертов и инцидентов в зависимости от ваших требований. По умолчанию период хранения алертов и инцидентов составляет 360 дней.

Дочерний тенант копирует период хранения алертов и инцидентов из родительского тенанта. При необходимости вы можете изменить период хранения алертов и инцидентов для дочернего тенанта.

Чтобы настроить период хранения алертов или инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите **Алерты и инциденты**.
4. В разделе **Срок хранения** укажите новый период хранения в одном или обоих полях:

   - **Срок хранения алерта (сут)**
   - **Срок хранения инцидента (сут)**

   Минимальное значение – `1`.
5. Нажмите на кнопку **Сохранить**.

Новый период хранения будет настроен.

Независимо от настроенного периода хранения, если истекший алерт связан с неистекшим инцидентом, алерт будет удален только после истечения периода хранения связанного инцидента. Если истекший инцидент имеет неистекшие связанные алерты, инцидент будет удален только после истечения периода хранения связанных алертов.

Если родительский инцидент, срок хранения которого истек, имеет дочерние инциденты, срок хранения которых не истек, родительский инцидент будет удален только после истечения срока хранения последнего дочернего инцидента.

Просмотр информации об активе

Детали актива – это окно, которое содержит всю информацию, связанную с активом.

Вы можете просмотреть детали актива одним из следующих способов:

- из деталей алерта;
- из деталей инцидента;
- из деталей события (если событие содержит активы);
- Из графа расследования.

Чтобы просмотреть сведения об активе:

1. В главном окне приложения перейдите в раздел **Мониторинг** и выполните одно из следующих действий:

   - Если вы хотите просмотреть детали активов из деталей алерта, нажмите **Алерты**, а затем в столбце **Идентификатор** нажмите на идентификатор алерта, которое включает актив, детали которого вы хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.

   - Если вы хотите просмотреть детали активов из деталей инцидента, нажмите **Инциденты**, а затем в столбце **Идентификатор** нажмите на идентификатор инцидента, который включает актив, детали которого вы хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.

   - Если вы хотите просмотреть детали активов из деталей события, нажмите **Поиск угроз**, а затем нажмите на событие, которое содержит актив, детали которого вы хотите просмотреть.

   - Если вы хотите просмотреть детали активов из графа расследования, нажмите **Инциденты**, а затем в столбце **Идентификатор** нажмите на идентификатор инцидента, который включает актив, детали которого вы хотите просмотреть. В открывшемся окне нажмите на кнопку **Посмотреть на графе**. Нажмите на узел алерта и в контекстном меню выберите пункт **Устройства** или **Пользователи**.

2. Выполните одно из следующих действий:

   - Нажмите на имя требуемого актива и в раскрывающемся списке выберите **Просмотреть свойства**.

   - На графе расследования нажмите на узел актива, а затем в контекстном меню выберите пункт **Просмотреть информацию**.

   Отображается окно с деталями актива.

В окне информации об активе вы можете переключаться между вкладками **Общие** и **Правила запрета**.

Вкладка Общие

Вкладка **Общая** содержит следующие разделы:

- **Свойства актива** – информация об активе, например название актива, идентификатор и тенант, которому принадлежит актив.

  Если действующая лицензия в KUMA включает AI-модуль, отображается поле **AI-оценка** и оценка актива. Это поле показывает степень нетипичной активности актива и может принимать значения в диапазоне от 0 до 1, где 0 – это ожидаемое поведение, 1 – это неожиданное поведение для актива в рамках инфраструктуры. Если приложение Kaspersky Endpoint Security со встроенным агентом установлено на активе (устройстве), отображается поле **Статус изоляции**. Вы можете просмотреть и изменить состояние сетевой изоляции устройства, перейдя по ссылке **Параметры** рядом со статусом.

- **Категории** – информация о категориях, связанных с активом.

- **Пользовательские поля** – поля активов, которые вы создали в Консоли KUMA.

- **Установленное программное обеспечение** – информация о программном обеспечении, установленном на активе.

  Вы можете использовать поле **Поиск**, чтобы быстро найти нужное приложение. Приложение отображается после того, как вы начинаете вводить любую информацию: название приложения, версию, производителя или дату установки.

- **KSC: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **Приложения "Лаборатории Касперского"** – информация о приложениях "Лаборатории Касперского", установленных на активе.

- **Состояние защиты устройства** – статус актива; возможны следующие значения: *OK*, *Критический*, *Предупреждение*. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **KICS for Networks: свойства активов** – информация об активе. Эта информация импортируется из KICS for Networks.

- **KICS for Networks: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.

Вы можете расширить разделы, нажав на значки (>) рядом с их названиями.

В панели инструментов вы можете выполнить следующие действия:

- Изменить информацию об активе, нажав на кнопку **Изменить**.

- Запустить действие по реагированию, нажав на кнопку **Реагирование** и выбрав в раскрывающемся списке действие по реагированию.

- Назначить категорию активу, нажав на кнопку **Привязать к категории**.

- Перейти в раздел **История реагирований**, раздел **Поиск угроз**, в список связанных алертов или список связанных инцидентов, нажав на кнопку **Открыть в** и выбрав в раскрывающемся списке, куда вы хотите перейти.

  В разделах **История реагирований** и **Поиск угроз** алерты или инциденты будут отфильтрованы по активу, в сведения которого вы перешли.

- Подключиться к активам с помощью удаленного терминала. Для этого нажмите на кнопку **Открыть удаленный терминал**.

- Экспортировать информацию об активах в CSV-файл, нажав на кнопку **Экспортировать в CSV**.

Вкладка правил запрета

Вкладка содержит таблицу правил запрета, примененных к устройству.

Правила запрета в таблице отображаются с одним из следующих статусов: **Применено, Применяется** или **Ошибка**.

Для просмотра списка правил запрета у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.

В таблице те же столбцы, что и в таблице в разделе Ресурсы и сервисы.

Вы можете просматривать и изменять параметры правил запрета. Для этого откройте свойства правила запрета, перейдя по ссылке с названием правила в столбце **Имя**. Откроется панель **Изменить правило запрета** на вкладке **Подробнее**. Вы можете изменить параметры правила запрета.

Также вы можете нажать на кнопку **Перейти в Поиск угроз**, чтобы просмотреть события, полученные при срабатывании правила запрета. На вкладке **Журнал изменений** вы можете просмотреть все изменения правила запрета.

Чтобы открыть сведения о правиле запрета, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
Если правило запрета принадлежит родительскому тенанту, к которому у вас не доступа, вы не сможете изменить правило запрета.

Исследование и реагирование с помощью удаленного терминала

Kaspersky EDR Expert позволяет подключиться к активу с помощью удаленного терминала. После подключения вы можете взаимодействовать с оболочкой операционной системы в режиме реального времени, чтобы исследовать алерты и инциденты, выполнять диагностику и реагировать на угрозы.

Через удаленный терминал вы можете управлять активом с помощью команд, поддерживаемых операционной системой, установленной на активе.

Используя удаленный терминал, вы можете подключаться к нескольким активам одновременно. В этом случае для каждого актива в Консоли OSMP открывается отдельное окно удаленного терминала.

Вы можете подключиться к активу с помощью удаленного терминала, если выполнены следующие условия:

- Вы активировали приложение по лицензии Kaspersky EDR Expert.
- У вас есть одна из следующих EDR-ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня.
- На активе установлено приложение Kaspersky Endpoint Security for Linux или Kaspersky Endpoint Security for Windows.

Вы не можете использовать удаленный терминал для подключения к активу, с которого вы получаете доступ к Консоли OSMP.

Если актив скомпрометирован, управление им через удаленный терминал может привести к непреднамеренному запуску вредоносного кода. Используйте удаленный терминал только для подключения к доверенным устройствам.

Управление подключениями удаленных терминалов

Вы можете использовать удаленный терминал для исследования угроз и реагирования на них в реальном времени.

Вы можете получить доступ к удаленному терминалу одним из следующих способов:

- Из деталей инцидента.
- Из деталей алерта.
- Из сведений об активе.
- Из таблицы активов (вкладка **Обнаружение и реагирование**).

Подключение к активам с помощью удаленного терминала

Чтобы подключиться к активам:

1. В главном окне приложения выполните одно из следующих действий:
   - Чтобы получить доступ к удаленному терминалу из деталей инцидента, перейдите в раздел **Мониторинг** → **Инциденты**. В таблице инцидентов нажмите на идентификатор нужного инцидента, а затем в открывшемся окне перейдите на вкладку **Активы**.
   - Чтобы получить доступ к удаленному терминалу из деталей алерта, перейдите в раздел **Мониторинг** → **Алерты**. В таблице алертов нажмите на идентификатор нужного алерта, а затем в открывшемся окне перейдите на вкладку **Активы**.

- Чтобы получить доступ к удаленному терминалу из сведений об активе, перейдите в раздел **Управление активами** → **Активы (Устройства)**. Выберите вкладку **Обнаружение и реагирование**, а затем в таблице активов нажмите на имя нужного актива. В контекстном меню нажмите **Подробнее**. В открывшейся панели сведений об активе нажмите на значок с многоточием (⋮).

- Чтобы получить доступ к удаленному терминалу из таблицы активов, перейдите в раздел **Управление активами** → **Активы (Устройства)**. Выберите вкладку **Обнаружение и реагирование**, а затем в таблице активов выберите нужный актив.

2. Нажмите на кнопку **Открыть удаленный терминал**.

3. Если требуется выполнить действия по реагированию с активом, выполните действия в следующем порядке:

   a. В открывшемся окне **Удаленный терминал** выполните одно из следующих действий:

   - Для устройств под управлением ОС Windows:

     ```
     response.exe
     ```

   - Для устройств под управлением ОС Linux:

     ```
     response
     ```

   b. Нажмите на клавишу **`Enter`**.

   c. Скопируйте пароль нажатием на ссылку **Копировать пароль**, затем вставьте пароль в удаленный терминал.

   После установления удаленного сеанса с активом вы можете исследовать угрозы и при необходимости выполнить действия по реагированию.

Все действия, выполняемые в удаленном терминале, регистрируются.

Если актив неактивен более 10 минут, подключение с ним прерывается.

Просмотр активных подключений в удаленном терминале

С помощью удаленного терминала вы можете подключаться и работать с несколькими активами одновременно. Если вы не завершили сеанс с активом вручную или срок действия сеанса не истек, сеанс останется активным, даже если вы перейдете в другой раздел Консоли OSMP.

Чтобы просмотреть активные сеансы удаленного терминала,

нажмите на **Количество подключений** в правом верхнем углу Консоли OSMP.

Откроется окно **Удаленный терминал**.

Отключение от активов с помощью удаленного терминала

Чтобы отключиться от активов,

в окне **удаленного терминала** нажмите на значок крестика (✕).

Если вы хотите отключиться от нескольких активов, нажмите на кнопку **Отключить все**.

Актив будет отключен от удаленного терминала.

Выполнение действий по реагированию с помощью удаленного терминала

После подключения к активу через удаленный терминал вы можете исследовать угрозы и реагировать на них с помощью интерфейса командной строки.

Для выполнения команд используется следующий синтаксис:

```
<common> <parameter> <argument> [--option=value] [--flag]
```

Обратите внимание, что флаги `--flag` представляют собой логические значения. Если флаг указан в команде, для него принимается значение `true`. Также можно явным образом задать значение `true` или `false`. Если флаг в команде не указан, для него принимается значение `false`. Флаг `--case-sensitive` является исключением из этого правила, его поведение подробнее описано ниже.

Общие параметры командной строки

Параметр	Тип	Описание
help	string	Открывает онлайн-справку.
task-timeout	целое число	Ограничивает время выполнения задачи (в секундах).
storage-path	string	Задает путь к файлам общего доступа для хранения результатов действий по реагированию.

Параметры действий по реагированию

Вы можете использовать следующие параметры в зависимости от действия по реагированию, которое вы хотите выполнить с активом:

Удалить файл

Чтобы удалить файл с устройства, используйте следующие параметры действия реагирования:

Параметр	Аргументы	Возможные значения	Тип	Описание
`delete-file`	[filePath]	`md5`	строка	MD5-хеш файла. Используется с путем к файлу. Может быть указан с или без SHA256.
		`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу. Может быть указан с или без MD5.
		`skip`	массив перечислений	Условия для невыполнения действия по реагированию. Возможные значения: • `self-defence` • `sco` • `kl-signed` • `kl-by-trusted-app`
		`with-subfolders`	флаг	Выполните рекурсивный поиск, если в параметре `filePath` указана директория.
		`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.

Пример

```
delete-file "C:/file path.txt" --md5=12345 --case-sensitive --skip=self-defence --skip=sco --skip=kl-signed --skip=kl-by-trusted-app
```

Управление службами

Это действие по реагированию доступно только на устройствах с операционной системой Windows.

Чтобы управлять службами на устройстве, используйте следующие параметры действия по реагированию:

Параметр	Аргументы	Возможные значения	Тип	Описание
`change-service`	[operationType] Возможные значения: • `start` • `stop` • `pause` • `resume` • `delete` • `change-startup-type`	`startup-type`	перечисление	Указывает тип запуска для операции `change-startup-type`. Этот параметр игнорируется для других операций. Возможные значения: • `Boot` • `System` • `Automatic` • `Manual` • `Disabled`
		`service-name`	строка	Имя службы. Маски поддерживаются.
		`md5`	строка	MD5-хеш файла. Может быть указан с или без SHA256.
		`sha256`	строка	SHA256-хеш файла. Может быть указан с или без MD5.

Пример

```
change-service change-startup-type --startup-type=auto --service-name=ServiceName --md5=12345
```

Перемещение файла на карантин

Чтобы предотвратить распространение угрозы, вы можете поместить зараженный файл на карантин. Для этого используйте следующие параметры действия по реагированию:

Параметр	Аргументы	Возможные значения	Тип	Описание
`quarantine-file`	[filePath]	`skip`	массив перечислений	Условия для невыполнения действия по реагированию. Возможные значения: • `self-defence` • `sco` • `kl-signed` • `kl-by-trusted-app`
		`legacy-file-id`	флаг	Если указан, возвращает устаревшие 64-разрядные идентификаторы карантина вместо идентификаторов GUID.
		`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.
		`delete`	флаг	Удаляет файл после помещения на карантин.
		`md5`	строка	MD5-хеш файла. Используется с путем к файлу. Может быть указан с или без SHA256.
		`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу. Может быть указан с или без MD5.

Пример

```
quarantine-file C:/filePath --skip=self-defence --skip=sco --skip=kl-signed --skip=kl-by-trusted-app
```

Удалить файл из карантина

Чтобы удалить зараженный файл из директории карантина на устройстве, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`delete-quarantined-file`	`file-id`	строка	Идентификатор файла на карантине.
	`legacy-file-id`	целое число	Идентификатор устаревшего карантина.

Пример

```
delete-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0
```

Восстановить файл из карантина

Если у вас есть основания полагать, что файл в карантине безопасен, вы можете восстановить файл на устройстве. Для этого используйте следующие параметры Действия по реагированию:

Параметр	Возможные значения	Тип	Описание
restore-quarantined-file	file-id	строка	Идентификатор файла на карантине.
	legacy-file-id	целое число	Идентификатор устаревшего карантина.
	replace	флаг	Заменяет существующий файл.
	remove	флаг	Удаляет файл из карантина после восстановления.
	destination	строка	Указывает путь назначения, используемый для восстановления объекта из резервной копии. Если путь не указан, объект восстанавливается по исходному пути.
	fallback-destination	строка	Задает резервный путь к точке назначения. Используется только в случае сбоя восстановления к первоначальному пути, поскольку путь не существует или доступ запрещен.

Пример

```
restore-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --replace --fallback-destination="C:/path"
```

Получение файла из карантина

Файл на карантине, находящийся на устройстве, можно получить из карантина для дальнейшего анализа. Чтобы получить файл из карантина, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
get-quarantined-file	file-id	строка	Идентификатор файла на карантине.
	legacy-file-id	целое число	Идентификатор устаревшего карантина.
	stream-index	целое число	Индекс потока файла для получения.

После завершения действия по реагированию полученный файл отобразится в Консоли OSMP в разделе **Файлы**.

Пример

```
get-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --stream-index=0
```

Завершение процессов

Чтобы завершить процессы на устройстве, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`terminate-process`	`path`	строка	Путь к исполняемому процессу.
	`pid`	целое число	Идентификатор системного процесса.
	`unique-pid`	целое число	Идентификатор процесса.
	`md5`	строка	MD5-хеш файла. Используется с путем к файлу. Может быть указан с или без SHA256.
	`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу. Может быть указан с или без MD5.
	`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.
	`expand-env`	флаг	Раскрывает переменные окружения в путях.
	`skip`	массив перечислений	Условия для невыполнения действия по реагированию. Возможные значения: • `self-defence` • `sco` • `kl-signed` • `kl-by-trusted-app`
	`limit`	integer	Максимальное количество попыток завершения процесса. Если значение не указано, количество попыток не ограничено.

Пример

```
terminate-process --pid=1234 --limit=100
```

Получить файл

Чтобы получить файл с устройства, используйте следующие параметры действия реагирования:

Параметр	Аргументы	Возможные значения	Тип	Описание
`get-file`	[filePath]	`md5`	строка	MD5-хеш файла. Используется с путем к файлу. Может быть указан с или без SHA256.
		`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу. Может быть указан с или без MD5.
		`max-size`	целое число	Максимальный размер файла в байтах. Действие по реагированию не выполняется, если файл превышает этот размер. По умолчанию размер не ограничен.
		`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.

После завершения действия по реагированию файл будет сохранен в защищенный паролем ZIP-архив. Пароль для файла архива – *infected*.

Пример

```
get-file C:/file --md5=1234567890 --max-size=1000 --case-sensitive
```

Включить сетевую изоляцию

Чтобы включить сетевую изоляцию для устройства, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`start-network-isolation`	`timeout`	целое число	Продолжительность сетевой изоляции. После истечения срока действия изоляция автоматически выключается. По умолчанию продолжительность изоляции не ограничена.
	`expand-env`	флаг	Раскрывает переменные окружения в путях.
	`no-notify-user`	флаг	Выключает уведомление пользователя об операции сетевой изоляции.
	`exclude`		Правило исключения сети. Этот параметр использовать отдельно невозможно. Чтобы настроить исключения, укажите один или несколько дочерних параметров: • `process` • `direction` • `remote-ip-v4` • `remote-ip-v6` • `local-port-from` • `local-port-to` • `remote-port-from` • `remote-port-to` • `protocol`
	`process`	string	Задает необязательный процесс приема или передачи. Значение должно быть полным путем к исполняемому файлу. Маски не поддерживаются. Переменные среды поддерживаются только в Windows.
	`direction`	перечисление	Задает направление подключения для протоколов на основе подключения (например, TCP) или направление пакета для протоколов на основе датаграмм (например, UDP). Если не указано иное, используются оба направления. Возможные значения: • `inbound` • `outbound` • `both`
	`remote-ip-v4`	строка	Удаленный IPv4-адрес в формате xxx.xxx.xxx.xxx. Поддерживаются префиксы подсети. Если не указан IPv4-адрес или IPv6-адрес, будет сопоставлен любой IP-адрес.
	`remote-ip-v6`	строка	Удаленный IPv6-адрес в формате xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. Поддерживаются префиксы подсети. Если не указан IPv4-адрес или IPv6-адрес, будет сопоставлен любой IP-адрес.
	`local-port-from`	целое число	Нижняя граница диапазона локальных портов. Если не граница указана, будет сопоставлен любой порт. Если порт не применим к пакетному протоколу, правило неактивно.
	`local-port-to`	целое число	Верхняя граница диапазона локальных портов. Если не граница указана, будет сопоставлен любой порт. Если порт не применим к пакетному протоколу, правило неактивно.
	`remote-port-from`	целое число	Нижняя граница диапазона удаленных портов. Если не граница указана, будет сопоставлен любой порт. Если порт не применим к пакетному протоколу, правило неактивно.
	`remote-port-to`	целое число	Верхняя граница диапазона удаленных портов. Если не граница указана, будет сопоставлен любой порт. Если порт не применим к пакетному протоколу, правило неактивно.
	`protocol`	целое число	Идентификатор протокола IANA, например TCP = 6. Если не граница указана, будет сопоставлен любой протокол.

Пример

```
start-network-isolation --timeout=300 exclude --process="C:/process.exe" exclude --local-port-from=1 --local-port-to=10 --direction=inbound --no-notifyuser
```

Выключить сетевую изоляцию

Чтобы выключить сетевую изоляцию для устройства, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`stop-network-isolation`	`no-notify-user`	флаг	Выключить сетевую изоляцию для устройства. По умолчанию пользователь получает уведомление, если сетевая изоляция выключена. Если указан параметр `--no-notify-user`, пользователь не получает уведомления. Параметр `--no-notify-user` доступен только на устройствах с операционной системой Windows.

Пример

```
stop-network-isolation --no-notify-user
```

Получить данные для расследования

Получение списка файлов

Чтобы получить список файлов и папок, хранящихся на диске, используйте следующие параметры действия реагирования.

Параметр	Возможные значения	Тип	Описание
`get-forensic files`	`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. Доступно только на устройствах с операционной системой Windows. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.
	`with-data-streams`	флаг	Указывает, включены ли Дополнительные потоки данных в отчет.
	`max-depth`	целое число	Максимальная глубина поиска. 0 означает неограниченную глубину. 1 выполняет поиск только в указанной директории.
	`max-files`	целое число	Максимальное число файлов или Дополнительных потоков данных для поиска. Поиск останавливается при достижении ограничения.
	`include-dir`	массив строк	Директории для включения в проверку. Пути к директориям могут содержать переменные среды (например, %TMP% или% TEMP%). Если пути не указаны, включаются все локальные директории.
	`exclude-dir`	массив строк	Директории, которые нужно добавить в исключения из проверки. Пути к директориям могут содержать переменные среды (например,%TMP% или% TEMP%).
	`include-files`	массив строк	Маски имен файлов для поиска (например, *.ps1). Если маски не указаны, будут включены все файлы.
	`exclude-files`	массив строк	Маски имен файлов, которые нужно исключить из поиска (например, *.ps1). Если маска не указана и указано значение `exclude-dir`, исключаются все файлы.

Пример

```
get-forensic files --max-depth=3 --max-files=1000 --include-dir="C:/include1" --include-dir=D:/include2
```

Получение списка процессов

Чтобы получить список процессов, запущенных на устройстве, выполните следующую команду:

```
get-forensic processes
```

Получение списка точек автозапуска

Чтобы получить список точек автозапуска, выполните следующую команду:

```
get-forensic autoruns
```

Получение дампа памяти процесса

Чтобы получить дамп памяти процесса, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`get-forensic process-dump`	`pid`	целое число	Идентификатор системного процесса.
	`unique-pid`	целое число	Уникальный идентификатор процесса.
	`md5`	строка	MD5-хеш файла. Используется с путем к файлу.
	`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу.

Пример

```
get-forensic process-dump --pid=123 --md5=abcdef123456
```

Получение файла дампа

Чтобы получить файл дампа, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`get-forensic files-dump`	`case-sensitive`	флаг	Указывает, чувствителен ли путь к регистру. По умолчанию зависит от файловой системы. Доступно только на устройствах с операционной системой Windows. Если флаг `--case-sensitive` не указан, задача наследует поведение операционной системы в отношении чувствительности к регистру и работает в режиме чувствительности к регистру. Чтобы запустить задачу в режиме нечувствительности к регистру, задайте `--case-sensitive=false`.
	`path`	array of string	Полные пути файлов дампов. Поддерживаются общие файлы и файлы метаданных (например, $Mft, $Boot). Маски не поддерживаются.
	`with-data-streams`	флаг	Указывает, включены ли Дополнительные потоки данных в отчет.
	`sha256`	строка	SHA256-хеш файла. Используется с путем к файлу.

Пример

```
get-forensic files-dump --path="C:/path1"--path="D:/path2" --with-data-streams
```

Получение ключа реестра

Доступно только на устройствах с операционной системой Windows.

Чтобы получить ключ реестра, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`get-forensic registry-dump`	`path`	array of string	Полные пути ключей реестра для создания файла дампа. Маски не поддерживаются.

Пример

```
get-forensic registry-dump --path="C:/path1" --path="D:/path2"
```

Получение информации о системе

Чтобы получить информацию о системе устройства, выполните следующую команду:

```
get-forensic system-info
```

Получение переменных среды

Доступно только на устройствах с операционной системой Windows.

Чтобы получить переменные среды, выполните следующую команду:

```
get-forensic environment-variables
```

Получение дампа памяти

Чтобы получить дамп памяти, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`get-forensic memory-dump`	`compress`	флаг	Указывает, сжимается ли дамп с помощью gzip с быстрым уровнем сжатия.
	`segment-size`	integer	Задает размер сегментов дампа в байтах. Дамп разбивается на сегменты указанного размера. Если значение равно 0 или не указано, дамп не разбивается.

Пример

```
get-forensic memory-dump --compress --segment-size=1000
```

Получение образа диска

Чтобы получить образ диска, используйте следующие параметры действия по реагированию:

Параметр	Возможные значения	Тип	Описание
`get-forensic disk-dump`	`logical`	строка	Имя логического диска в формате, зависящем от операционной системы (например, C:, D:, E: в Windows).
	`physical`	строка	Имя физического диска в формате, зависящем от операционной системы (например, \\.\PHYSICALDRIVE0 в Windows).
	`compress`	флаг	Указывает, сжимается ли дамп с помощью gzip с быстрым уровнем сжатия.
	`segment-size`	integer	Задает размер сегментов дампа в байтах. Дамп разбивается на сегменты указанного размера. Если значение равно 0 или не указано, дамп не разбивается.

Пример

```
get-forensic disk-dump --logical="C:" --segment-size=1000 --compress
```

Поиск угроз

Страница **Поиск угроз** содержит инструменты, которые помогают анализировать события для поиска угроз и уязвимостей, которые не были обнаружены автоматически. Чтобы создать алерт из набора событий, выберите события и нажмите на кнопку **Создать алерт**.

Вы можете открыть страницу **Поиск угроз** любым из следующих способов:

- В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.
- В деталях алерта или инцидента в контекстном меню выберите пункт **Поиск в разделе Поиск угроз**.
- В сведениях об инциденте нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на кнопку **Поиск угроз**.

На странице **Поиск угроз** отображаются события. Вы можете отфильтровать события:

- изменив SQL-запрос;
- изменив период;
- выбрав тенант, которому принадлежат события.

Модель данных событий

Приложения Endpoint Agent отправляют в OSMP информацию о следующих событиях:

- Процесс
- File Create
- File Modify
- File Rename
- File Read
- File Delete
- File Attributes Modify
- File Creation Time Modify
- File Hardlink Created
- File Symlink Created
- Module
- Registry Create

- Registry Delete
- Registry Modify
- Registry Rename
- Registry Query
- Registry Save
- Connection
- Port Listen
- AMSI Scan
- Process Console Input
- Driver
- Process Interpreted File Run
- DNS
- Pipe Create
- Pipe Connect
- LDAP
- WMI Activity
- WMI Consumer Registered
- Code Injection
- Process Access
- Threat Detect
- Threat Detect Processing Result
- Linux Event Log
- Windows Event Log
- Blocked Document
- Applock
- Process Terminated
- Устройство
- File System Mount

- File System Unmount
- Bits Job Create (новое в версии 8.0)
- Bits Job Complete (новое в версии 8.0)
- Bits Job Start (новое в версии 8.0)
- Bits Job Stop (новое в версии 8.0)
- Bits Job Add File (новое в версии 8.0)
- Bits Job Error (новое в версии 8.0)
- Service Create (новое в версии 8.0)
- Service Modify (новое в версии 8.0)
- Service Delete (новое в версии 8.0)
- Scheduled Task Create (новое в версии 8.0)
- Scheduled Task Modify (новое в версии 8.0)
- Scheduled Task Delete (новое в версии 8.0)
- File Owner Change (новое в версии 8.0)
- Изменение списка управления доступом к файлу (новое в версии 8.0)
- Изменение владельца реестра (новое в версии 8.0)
- Registry ACL Change (новое в версии 8.0)
- Executable Memory Mapped (новое в версии 8.0)
- Agent Start (новое в версии 8.0)
- Agent Stop (новое в версии 8.0)
- Agent Install (новое в версии 8.0)
- Agent Uninstall (новое в версии 8.0)
- Agent Action (новое в версии 8.0)
- System Startup (новое в версии 8.0)
- System Shutdown (новое в версии 8.0)
- Connection Close (новое в версии 8.0)

Включение события `Connection Close` может привести к значительному увеличению использования ресурсов на защищаемых устройствах.

Process

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Process

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessCalltrace	string	Трассировка стека функций вызова процесса
ProcessFileLnkName	string	Имя LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса

Поле	Тип	Описание
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен

Поле	Тип	Описание
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Create

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш содержимого файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс

Поле	Тип	Описание
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полный путь к файлу исполняемого процесса
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип исполняемого файла процесса
ProcessFileUrl	string	URL, с которого был загружен исполняемый файла процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)

Поле	Тип	Описание
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла
ParentProcessFileSignSubjectname	string	Имя субъекта сертификата, которым был подписан файл
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Список флагов прародительского процесса
GrandParentProcessDirectory	string	Текущая рабочая директория прародительского процесса. Указывается для Linux и macOS
GrandParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла прародительского процесса
GrandParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserRealname	string	Реальное имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Реальное имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Идентификатор эффективной группы пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла)
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл прародительского процесса
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время, когда файл был подписан
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Modify

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события File Modify

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере

Поле	Тип	Описание
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла

Поле	Тип	Описание
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Rename

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события File Rename

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
FileOldName	string	Предыдущее имя файла
FileOldPath	string	Предыдущий путь к файлу
FileOldFullname	string	Предыдущий полный путь к файлу
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса

Поле	Тип	Описание
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла

Поле	Тип	Описание
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd

Поле	Тип	Описание
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса

Поле	Тип	Описание
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Read

Этот тип событий поддерживается в операционных системах Windows и Linux (в Linux только для версий, поддерживающих eBPF).

Поля события File Read

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки

Поле	Тип	Описание
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"

Поле	Тип	Описание
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса

Поле	Тип	Описание
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS

Поле	Тип	Описание
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS

Поле	Тип	Описание
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Delete

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс

Поле	Тип	Описание
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)

Поле	Тип	Описание
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Attributes Modify

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события File Attributes Modify

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере

Поле	Тип	Описание
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла

Поле	Тип	Описание
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Creation Time Modify

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileDelafterreboot	string	Истина, если файл будет удален после перезагрузки. Указывается для операции удаления. Указывается только для Windows
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)

Поле	Тип	Описание
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс

Поле	Тип	Описание
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Hardlink Created

Этот тип событий поддерживается в операционных системах Windows.

Поля события File Hardlink Created

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileTargetName	string	Имя конечного объекта. Используется в событиях типа Filechange
FileTargetPath	string	Путь к конечному объекту. Используется в событиях типа Filechange
FileTargetFullname	string	Имя и путь конечного объекта. Используется в событиях типа Filechange
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)

Поле	Тип	Описание
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса

Поле	Тип	Описание
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false

Поле	Тип	Описание
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Symlink Created

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileTargetName	string	Имя конечного объекта. Используется в событиях типа Filechange
FileTargetPath	string	Путь к конечному объекту. Используется в событиях типа Filechange
FileTargetFullname	string	Имя и путь конечного объекта. Используется в событиях типа Filechange
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса

Поле	Тип	Описание
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)

Поле	Тип	Описание
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса

Поле	Тип	Описание
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Module

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileSize	int	Размер файла в байтах

Поле	Тип	Описание
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileAttr	int	Атрибуты файловой системы
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileType	string	Тип файла
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
FileHijackingpath	string	Путь к оригинальной DLL
DotnetFileAssemblyName	string	Полное имя сборки .NET. Содержит хэш сертификата (используется для фильтрации)
DotnetFileAssemblyFlags	int	Флаги сборки .NET
DotnetFileModuleFlags	int	Флаги модуля сборки .NET
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла

Поле	Тип	Описание
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса

Поле	Тип	Описание
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Create

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Create

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)

Поле	Тип	Описание
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
RegValueType	string	Тип значения реестра
RegValueData	string	Данные в значении реестра
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Delete

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Delete

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса

Поле	Тип	Описание
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс

Поле	Тип	Описание
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Modify

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Modify

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
RegValueType	string	Тип значения реестра
RegValueData	string	Данные в значении реестра
RegOldValueData	string	Предыдущие данные в значении реестра
RegOldValueMd5	string	Предыдущее значение MD5 хеша файла из параметра RegValueData
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса

Поле	Тип	Описание
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса

Поле	Тип	Описание
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса

Поле	Тип	Описание
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс

Поле	Тип	Описание
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductvendor	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	

Registry Rename

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Rename

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
RegValueType	string	Тип значения реестра
RegValueData	string	Данные в значении реестра
RegOldKeyName	string	Предыдущее имя ключа реестра
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)

Поле	Тип	Описание
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Query

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Query

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события

Поле	Тип	Описание
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
RegValueType	string	Тип значения реестра
RegValueData	string	Данные в значении реестра
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса

Поле	Тип	Описание
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Save

Этот тип событий поддерживается в операционных системах Windows.

Поля события Registry Save

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)

Поле	Тип	Описание
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были затронуты событием
RegValueName	string	Имя значения реестра
RegValueType	string	Тип значения реестра
RegValueData	string	Данные в значении реестра
FileFullname	string	Полный путь к файлу
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса

Поле	Тип	Описание
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Connection

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Connection

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
NetSrcIp	string	Адрес источника ipv4/ipv6
NetSrcPort	int	Номер порта источника
NetDstIp	string	Адрес назначения ipv4/ipv6
NetDstPort	int	Номер порта назначения
NetUrlHostname	string	Имя удаленного хоста
NetUrlPort	int	Порт удаленного хоста
NetUri	string	URI назначения для HTTP
NetHttpMethod	string	Метод HTTP
NetHttpUseragent	string	Строка-идентификатор с информацией о клиентской программе, инициировавшей запрос
NetHttpReferrer	string	Поле заголовка HTTP, которое определяет адрес веб-страницы, с которой был запрошен ресурс
NetProtocol	string	IP-протокол
NetDirection	string	Направление сетевого соединения (входящее, исходящее)
NetHttpHeaderName	string	Имя HTTP-заголовка
NetHttpHeaderValue	string	Значение HTTP-заголовка
NetRaw	string	Флаг, использовался ли сырой сокет
NetTlsVersion	string	Версия TLS
NetTlsSni	string	Указание имени сервера TLS
NetTlsSniEncrypted	string	Указание зашифрованного имени сервера TLS
NetTlsCertificateMd5	string	MD5-хэш сертификата TLS
NetTlsCertificateSha1	string	SHA1 хэш сертификата TLS
NetTlsCertificateSubjectname	string	Альтернативное имя субъекта TLS (SAN)
NetTlsCertificateIssuername	string	Имя эмитента сертификата TLS
NetTlsCertificateSerialnumber	string	Серийный номер сертификата TLS
NetTlsCertificateCheckresult	string	Результат проверки сертификата TLS
NetTlsCertificateValidfrom	int	Дата начала срока действия сертификата TLS
NetTlsCertificateValidto	int	Дата окончания срока действия сертификата TLS
NetTlsCiphersuite	int	Поддерживаемые алгоритмы TLS
NetTlsJa3	string	Ja3 отпечаток, используемый в TLS
NetTlsJa3s	string	Ja3s отпечаток, используемый в TLS
NetTlsJa3Md5	string	MD5-хэш отпечатка Ja3 сертификата TLS
NetTlsJa3sMd5	string	MD5-хэш отпечатка Ja3s сертификата TLS
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса

Поле	Тип	Описание
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс

Поле	Тип	Описание
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd

Поле	Тип	Описание
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса

Поле	Тип	Описание
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Port Listen

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Port Listen

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события

Поле	Тип	Описание
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
NetDstIp	string	Адрес назначения ipv4/ipv6
NetDstPort	int	Номер порта назначения
NetProtocol	int	IP-протокол
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс

Поле	Тип	Описание
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS

Поле	Тип	Описание
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

AMSI Scan

Этот тип событий поддерживается в операционных системах Windows.

Поля события AMSI Scan

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)

Поле	Тип	Описание
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
AmsiContentType	string	Тип объекта, который был отправлен на сканирование AMSI
AmsiContentData	string	Содержимое объекта, обнаруженного при AMSI- сканировании
AmsiContentName	string	Имя объекта, отправленного на AMSI-сканирование
AmsiContentMd5	string	MD5 объекта, отправленного на AMSI-сканирование
AmsiContentSha256	string	SHA256 объекта, отправленного на AMSI-сканирование
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса

Поле	Тип	Описание
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение

Поле	Тип	Описание
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Process Console Input

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Process Console Input

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
InputText	string	Текст интерактивного ввода
InputType	string	Тип объекта ввода
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс

Поле	Тип	Описание
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен

Поле	Тип	Описание
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Driver

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла

Поле	Тип	Описание
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение

Process Interpreted File Run

Этот тип событий поддерживается в операционных системах Windows.

Поля события Process Interpreted File Run

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события

Поле	Тип	Описание
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла без пути, который выполняется процессом интерпретатором
FilePath	string	Путь к файлу (без его имени), который выполняется процессом интерпретатором
FileFullname	string	Полный путь к файлу, который выполняется процессом интерпретатором
FileSize	int	Размер файла (в байтах), выполняемого интерпретатором
FileCreationtime	int	Дата и время создания файла, который выполняется интерпретатором
FileModificationtime	int	Время последней модификации файла, который выполняется процессом интерпретатором
FileAttrModificationtime	int	Время последнего изменения атрибутов файла, который выполняется интерпретатором
FileMd5	string	MD5 хэш файла, который выполняется процессом интерпретатором
FileSha256	string	SHA256 хэш файла, который выполняется процессом интерпретатором
FileAttr	int	Список атрибутов файловой системы для файла, который выполняется интерпретатором
FileType	string	Тип файла, который выполняется процессом интерпретатором
FileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла, выполняемого процессом интерпретатором
FileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
FileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO файла, выполняемого интерпретатором
FileDescription	string	Описание, указанное в ресурсе VERSIONINFO
FileOriginalname	string	Оригинальное имя файла, выполняемого интерпретатором, указанное в ресурсе VERSIONINFO
FileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл, выполняемый интерпретатором
FileSignResult	string	Результат проверки подписи файла, выполняемого интерпретатором: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла, выполняемого интерпретатором

Поле	Тип	Описание
FileUrl	string	URL адрес, с которого был загружен файл, который выполняется процессом интерпретатором
FileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл, который выполняется интерпретатором
FileOwnerUserId	int	Идентификатор пользователя - владельца файла, выполняемого интерпретатором. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла, выполняемого интерпретатором. Указывается для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы владельцев файла, выполняемого интерпретатором. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы владельцев файла, выполняемого интерпретатором. Указано для Linux и macOS
FileCapPermitted	string	Набор разрешённых возможностей файла, который выполняется интерпретатором
FileCapInheritable	string	Наследуемые возможности файла, который выполняется интерпретатором
FileCapEffective	string	Эффективные возможности файла, который выполняется интерпретатором
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)

Поле	Тип	Описание
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса

Поле	Тип	Описание
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd

Поле	Тип	Описание
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс

Поле	Тип	Описание
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

DNS

Этот тип событий поддерживается в операционных системах Windows и Linux (в Linux только для внешних сетевых соединений).

Поля события DNS

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB

Поле	Тип	Описание
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
DnsServerIp	string	Запрашиваемый DNS-сервер
DnsQueryOptions	string	Параметры выполненного DNS-запроса
DnsQueryStatus	int	Код ошибки при выполнении операции
DnsResourceName	string	Запрашиваемый при DNS-запросе URL
DnsResourceType	string	Тип выполняемого DNS-запроса
DnsAnswer	string	Результат DNS-запроса
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса

Поле	Тип	Описание
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS

Поле	Тип	Описание
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS

Поле	Тип	Описание
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Pipe Create

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
PipeName	string	Имя именованного канала, который был создан или с которым было установлено соединение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса

Поле	Тип	Описание
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета

Поле	Тип	Описание
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Pipe Connect

Этот тип событий поддерживается в операционных системах Windows.

Поля события Pipe Connect

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере

Поле	Тип	Описание
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
PipeName	string	Имя именованного канала, который был создан или с которым было установлено соединение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса

Поле	Тип	Описание
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

LDAP

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
LdapSearchScope	string	Область или диапазон дерева каталогов, в котором следует выполнить поиск LDAP
LdapSearchFilter	string	Условия или критерии, которые поисковый запрос LDAP будет использовать для сопоставления записей в каталоге
LdapSearchDn	string	Начальная точка или база в дереве каталога, с которой начнется операция поиска в LDAP

Поле	Тип	Описание
LdapSearchAttr	string	Список определенных атрибутов, которые используются для фильтрации или поиска в LDAP
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс

Поле	Тип	Описание
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса

Поле	Тип	Описание
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

WMI Activity

Этот тип событий поддерживается в операционных системах Windows за исключением Windows XP.

Поля события WMI Activity

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки

Поле	Тип	Описание
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Protected host ID in the MDR solution
HostOsmpId	string	List of identifiers for OSMP Based XDR solution servers associated with the protected host
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
WmiRemote	string	Флаг удаленной операции WMI
WmiHostName	string	Имя узла-источника WMI-активности
WmiUserName	string	Имя учетной записи пользователя, выполнившего операцию WMI
WmiNamespacename	string	Пространство имен WMI, которое было запрошено
WmiQuery	string	Запрос WMI
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс

Поле	Тип	Описание
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса

Поле	Тип	Описание
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)

Поле	Тип	Описание
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

WMI Consumer Register

Этот тип событий поддерживается в операционных системах Windows за исключением Windows XP.

Поля события WMI Consumer Register

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки

Поле	Тип	Описание
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
WmiNamespacename	string	Пространство имен WMI, которое было запрошено
WmiFiltername	string	Имя фильтра, используемого потребителем событий
WmiConsumerName	string	Имя созданного потребителя событий
WmiConsumerText	string	MOF-код потребителя событий
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)

Поле	Тип	Описание
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)

Поле	Тип	Описание
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCreationtime	int	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileModificationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Code Injection

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Code Injection

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере

Поле	Тип	Описание
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
TargetProcessUniqueid	int	Уникальный идентификатор целевого процесса
TargetProcessId	int	Идентификатор целевого процесса (PID)
TargetProcessCmdline	string	Аргументы командной строки, передаваемые целевому процессу
TargetProcessFileName	string	Имя исполняемого файла целевого процесса (процесса, в котором была выполнена инъекция кода)
TargetProcessFilePath	string	Полный путь без имени файла к исполняемому файлу целевого процесса (процесса, в котором была осуществлена инъекция кода)
TargetProcessFileFullname	string	Полный путь к исполняемому файлу целевого процесса (процесса, в котором была осуществлена инъекция кода)
TargetProcessFileMd5	string	MD5 исполняемого файла целевого процесса
TargetProcessFileSha256	string	SHA256 исполняемого файла целевого процесса
TargetProcessIntegritylevel	int	Уровень целостности целевого процесса
TargetProcessFileUrl	string	URL, с которого был загружен исполняемый файл целевого процесса
TargetProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл целевого процесса был получен в виде вложения
TargetProcessFileAttr	int	Последнее время, когда атрибуты исполняемого файла целевого процесса были изменены
SyscallArgs	string	Аргументы системных вызовов
ProcessCalltrace	string	Трассировка стека функций вызова процесса
ProcessModifiedcmdline	string	Командная строка процесса
InjectMethod	string	Метод инъекции
InjectAddress	string	Поле содержит информацию об адресе, с которого начинается выполнение после инъекции
InjectImageFileName	string	Имя исходного исполняемого файла. Только для SET_WINDOWS_HOOK
InjectImageFileFullname	string	Имя и путь исходного исполняемого файла. Только для SET_WINDOWS_HOOK
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса

Поле	Тип	Описание
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла

Поле	Тип	Описание
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS

Поле	Тип	Описание
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса

Поле	Тип	Описание
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Process Access

Этот тип событий поддерживается в операционных системах Windows.

Поля события Process Access

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
AccessOperationtype	string	Тип операции доступа, выполняемый с хэндлом процесса (один процесс выполняет по отношению к другому процессу).
AccessRights	string	Желаемые права доступа к объекту процесса
ProcessCalltrace	string	Трассировка стека функций вызова процесса
TargetProcessFileName	string	Имя исполняемого файла целевого процесса (процесса, в котором была выполнена инъекция кода)
TargetProcessFilePath	string	Полный путь без имени файла к исполняемому файлу целевого процесса (процесса, в котором была осуществлена инъекция кода)
TargetProcessFileFullname	string	Полный путь к исполняемому файлу целевого процесса (процесса, в котором была осуществлена инъекция кода)
TargetProcessFileMd5	string	MD5 исполняемого файла целевого процесса
TargetProcessFileSha256	string	SHA256 исполняемого файла целевого процесса
TargetProcessFileCreationtime	int	Время создания исполняемого файла целевого процесса
TargetProcessFileModificationtime	int	Время последней модификации исполняемого файла целевого процесса

Поле	Тип	Описание
TargetProcessFileAttrModificationtime	int	Последнее время, когда атрибуты исполняемого файла целевого процесса были изменены
TargetProcessFileSize	int	Размер исполняемого файла целевого процесса в байтах
TargetProcessUniqueid	int	Уникальный идентификатор целевого процесса
TargetProcessId	int	Идентификатор целевого процесса (PID)
TargetProcessCmdline	string	Аргументы командной строки, передаваемые целевому процессу
TargetProcessFileUrl	string	URL, с которого был загружен исполняемый файл целевого процесса
TargetProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл целевого процесса был получен в виде вложения
TargetProcessFileAttr	int	Последнее время, когда атрибуты исполняемого файла целевого процесса были изменены
HandleProcessSrcFileName	string	Имя процесса, из которого был дублирован хэндл
HandleProcessSrcFilePath	string	Полный путь без имени файла процесса, из которого был дублирован хэндл
HandleProcessSrcFileFullname	string	Полный путь процесса, из которого был дублирован хэндл
HandleProcessSrcFileMd5	string	MD5 процесса, из которого был дублирован хэндл
HandleProcessSrcFileSha256	string	SHA256 процесса, из которого был дублирован хэндл
HandleProcessSrcFileCreationtime	int	Время создания процесса, из которого был дублирован хэндл
HandleProcessSrcFileModificationtime	int	Время последней модификации процесса, из которого был дублирован дескриптор
HandleProcessSrcFileAttrModificationtime	int	Время последней модификации атрибутов процесса, из которого был дублирован дескриптор
HandleProcessSrcFileSize	int	Размер исполняемого файла процесса, из которого был дублирован дескриптор
HandleProcessSrcUniqueid	int	Уникальный PID процесса, из которого был дублирован дескриптор
HandleProcessSrcId	int	Идентификатор процесса (PID) процесса, из которого был дублирован дескриптор
HandleProcessSrcIntegritylevel	int	Уровень целостности процесса, из которого был дублирован дескриптор
HandleProcessSrcCmdline	string	Параметры командной строки процесса, из которого был дублирован дескриптор
HandleProcessSrcFileUrl	string	URL, с которого был загружен исходный процесс
HandleProcessSrcFileEmailSrcAddress	string	Адрес отправителя, от которого в качестве вложения был получен исполняемый файл исходного процесса
HandleProcessDstFileName	string	Имя процесса, которому был продублирован дескриптор
HandleProcessDstFilePath	string	Полный путь без имени файла процесса, которому был продублирован дескриптор
HandleProcessDstFileFullname	string	Полный путь процесса, которому был продублирован дескриптор
HandleProcessDstFileMd5	string	MD5 процесса, которому был продублирован дескриптор
HandleProcessDstFileSha256	string	SHA256 процесса, которому был продублирован дескриптор
HandleProcessDstFileCreationtime	int	Время создания процесса, которому был продублирован дескриптор
HandleProcessDstFileModificationtime	int	Время последней модификации время процесса, которому был продублирован дескриптор
HandleProcessDstFileAttrModificationtime	int	Время последней модификации атрибутов процесса, которому был продублирован дескриптор
HandleProcessDstFileSize	int	Размер исполняемого файла процесса, которому был продублирован дескриптор
HandleProcessDstUniqueid	int	Уникальный PID процесса, которому был продублирован дескриптор
HandleProcessDstId	int	Идентификатор процесса (PID) процесса, которому был продублирован дескриптор
HandleProcessDstIntegritylevel	int	Уровень целостности процесса, которому был продублирован дескриптор
HandleProcessDstCmdline	string	Параметры командной строки процесса, которому был продублирован дескриптор

Поле	Тип	Описание
HandleProcessDstFileUrl	string	URL, с которого был загружен исходный процесс
HandleProcessDstFileEmailSrcAddress	string	Адрес отправителя, от которого в качестве вложения был получен исполняемый файл исходного процесса
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла

Поле	Тип	Описание
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение

Поле	Тип	Описание
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Threat Detect

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Threat Detect

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки

Поле	Тип	Описание
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
ThreatObjectFullname	string	Полный путь к файлу
ThreatObjectMd5	string	MD5-хэш содержимого файла
ThreatObjectSha256	string	SHA256 хэш содержимого файла
ThreatObjectType	string	Тип обнаруженного объекта
ThreatVerdictname	string	Название вердикта обнаруженной угрозы
ThreatRecordid	int	Идентификатор рекорды, сработавшей на угрозу
ThreatDatabaseTimestamp	int	Дата и время последнего обновления баз модуля антивирусной защиты
ThreatProcessingmode	int	Режим обработки, при котором был обнаружен объект
ThreatSilent	string	Статус вердикта обнаруженной угрозы
NetProtocol	int	IP-протокол
NetDstIp	string	Адрес назначения ipv4/ipv6
NetDstPort	int	Номер порта назначения
NetSrcIp	string	Адрес источника ipv4/ipv6
NetSrcPort	int	Номер порта источника
ThreatEmailAddress	string	Email адрес отправителя, от которого обнаруженный файл был получен в качестве вложения
ThreatEmailDestination	string	Email адрес получателя файла, распознанного модулем антивирусной защиты как угроза
ThreatEmailSubject	string	Тема письма, во вложении которого был получен файл, распознанный модулем антивирусной защиты как угроза

Поле	Тип	Описание
ThreatEmailMessageid	string	Уникальный идентификатор сообщения, в котором модулем антивирусной защиты была обнаружена угроза
ThreatEmailReceivedtimestamp	string	Время получения email-письма, в котором модулем антивирусной защиты была обнаружена угроза
ThreatDownloaderFileFullname	string	Путь к исполняемому файлу процесса, загрузившего файл, обнаруженный модулем антивирусной защиты
AmsiContentType	string	Тип объекта, который был отправлен на сканирование AMSI
AmsiContentData	string	Содержимое объекта, обнаруженного при AMSI- сканировании
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса

Поле	Тип	Описание
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).

Поле	Тип	Описание
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Threat Detect Processing Result

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
ThreatObjectFullname	string	Полный путь к файлу
ThreatObjectMd5	string	MD5-хэш содержимого файла
ThreatObjectSha256	string	SHA256 хэш содержимого файла
ThreatObjectType	string	Тип обнаруженного объекта

Поле	Тип	Описание
ThreatVerdictname	string	Название вердикта обнаруженной угрозы
ThreatRecordid	int	Идентификатор рекорды, сработавшей на угрозу
ThreatDatabaseTimestamp	int	Дата и время последнего обновления баз модуля антивирусной защиты
ThreatProcessingmode	int	Режим обработки, при котором был обнаружен объект
NetProtocol	int	IP-протокол
NetDstIp	string	Адрес назначения ipv4/ipv6
NetDstPort	int	Номер порта назначения
NetSrcIp	string	Адрес источника ipv4/ipv6
NetSrcPort	int	Номер порта источника
ThreatEmailAddress	string	Email адрес отправителя, от которого обнаруженный файл был получен в качестве вложения
ThreatDownloaderFileFullname	string	Путь к исполняемому файлу процесса, загрузившего файл, обнаруженный модулем антивирусной защиты
ThreatAction	string	Тип действия, предпринятого над объектом, распознанного модулем антивирусной защиты как угроза
ThreatActionresult	string	Результат действия, предпринятого над объектом, распознанным модулем антивирусной защиты как угроза. Из поля ThreatAction
ThreatActionreason	string	В случае успешного действия поле содержит 0. В случае неуспешного действия поле содержит причину неудачи
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса

Поле	Тип	Описание
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS

Поле	Тип	Описание
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса

Поле	Тип	Описание
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Linux Event Log

Этот тип событий поддерживается в операционных системах Linux.

Поля события Linux Event Log

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
LinuxEventType	string	Тип события
LinuxEventMessage	string	Сообщение из лога событий
LinuxOperationResult	string	Результат операции - например, успех или неудача
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса

Поле	Тип	Описание
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен

Поле	Тип	Описание
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Windows Event Log

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
SystemLogEventXml	string	XML события журнала Windows
SystemLogEventId	int	Идентификатор события журнала Windows
SystemLogChannelName	string	

Поле	Тип	Описание
SystemLogProviderName	string	
WinBinary	string	Атрибуты обрабатываемого объекта
WinData	string	Основные данные события Windows Event Log
WinAccessGranted	string	Параметры безопасности из событий в windows event log
WinAccessList	string	Права доступа, которыми обладает обрабатываемый объект
WinAccessMask	string	Права доступа, которыми обладает обрабатываемый объект
WinAccessReason	string	Причина, по которой файл помещен в категорию
WinAccessRemoved	string	Права доступа, которые были удалены с объекта
WinAccountDomain	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinAccountExpires	string	Параметры объектов active directory
WinAccountName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinAccountSessionIdentifier	string	Идентификатор сессии аутентификации в событии Network Policy Server
WinAction	string	Действие системы или безопасности в событии
WinActionID	string	Идентификатор действия, выполненного при событии
WinActionName	string	Название действия, выполненного при событии
WinActiveProfile	string	Активный профиль конфигурации или сети
WinAddedCAPs	string	Список добавленных централизованных политик доступа
WinAdditionalActionsID	string	Идентификаторы дополнительных действий, связанных с событием
WinAdditionalActionsString	string	Описание или строки дополнительных действий, связанных с событием
WinAdditionalDetails	string	Текст запроса
WinAdditionalInfo	string	Дополнительная информация о событии или объекте
WinAdditionalInfo2	string	Дополнительная информация о событии или объекте (второе поле)
WinAdvancedOptions	string	Расширенные параметры настройки
WinAlgorithmName	string	Название используемого криптографического алгоритма
WinAllowedToDelegateTo	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinAppCorrelationID	string	Код типа объекта
WinApplication	string	Имя обрабатываемого объекта
WinAppName	string	Название по
WinAppVersion	string	Версия компонента по
WinAsIsCAPs	string	Список неизмененных центральных политик доступа
WinAttributeLDAPDisplayName	string	Атрибуты обрабатываемого исполняемого файла
WinAttributes	string	Атрибуты объекта или события
WinAttributeSyntaxOID	string	Атрибуты обрабатываемого объекта
WinAttributeValue	string	Атрибуты обрабатываемого исполняемого файла
WinAuditPolicyChanges	string	Параметры безопасности из событий в windows event log
WinAuditSourceName	string	Имя обрабатываемого объекта
WinAuditStatusCode	string	Код статуса аудита события
WinAuthenticationLevel	string	Уровень аутентификации для запроса или соединения
WinAuthenticationPackageName	string	Имя обрабатываемого объекта

Поле	Тип	Описание
WinAuthenticationProvider	string	Поставщик аутентификации для события
WinAuthenticationServer	string	Сервер, выполнявший аутентификацию
WinAuthenticationService	string	Служба аутентификации, использованная в событии
WinAuthenticationType	string	Тип аутентификации для события
WinBackupType	string	Тип резервного копирования
WinBcdCCID	string	Параметры и свойства устройств класса смарт-карта
WinBMaxSlotIndex	string	Параметры и свойства устройств класса смарт-карта
WinBNumClockSupported	string	Параметры и свойства устройств класса смарт-карта
WinBNumDataRateSupported	string	Параметры и свойства устройств класса смарт-карта
WinBootMode	string	Параметры пользовательских сессий из событий в windows event log
WinBuildVersion	string	Версия отправляемой статистики
WinBVoltageSupport	string	Параметры и свойства устройств класса смарт-карта
WinCalledStationID	string	Идентификатор вызываемой станции в аутентификации
WinCallerProcessId	string	Идентификатор родительского процесса в системе (pid)
WinCallerProcessName	string	Имя обрабатываемого объекта
WinCallingStationID	string	Идентификатор вызывающей станции в аутентификации
WinCalloutKey	string	Ключ вызываемой функции или правила
WinCalloutName	string	Название вызываемой функции или правила
WinCategoryId	string	Параметры операций из событий в windows event log
WinCategoryName	string	Категория события или угрозы
WinCertificateTemplate	string	Шаблон сертификата, используемый в событии
WinCertIssuerName	string	Наименование эмитента сертификата
WinCertSerialNumber	string	Серийный номер сертификата
WinCertThumbprint	string	Отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования
WinChangeType	string	Тип внесенного изменения
WinClassId	string	Код типа объекта
WinClassName	string	Имя обрабатываемого объекта
WinClientAddress	string	Локальный ip адрес
WinClientIPAddress	string	IP-адрес клиента, инициировавшего событие
WinClientName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinClientProcessId	string	Идентификатор процесса клиента
WinClientProcessStartKey	string	Уникальный ключ процесса, создавшего задачу
WinCommandLine	string	Командная строка запущенного процесса
WinCompatibleIds	string	Дополнительные параметры событий в windows event log
WinComputerAccountChange	string	Параметры операций из событий в windows event log
WinComputerName	string	Имя компьютера, где произошло событие
WinConditions	string	Условия, связанные с событием или фильтром
WinConfigAccessPolicy	string	Политика доступа к конфигурации
WinConfiguredNames	string	Настроенные имена ресурсов или объектов
WinContextInfo	string	Параметры задач, зарегистрированных в событиях в windows event log

Поле	Тип	Описание
WinCountOfCredentialsReturned	string	Количество возвращенных учетных данных
WinCrashOnAuditFailValue	string	Значение настройки аварийного завершения при сбое аудита
WinCredType	string	Тип учетных данных
WinCurrentEngineVersion	string	Текущая версия движка защиты
WinCurrentSignatureVersion	string	Текущая версия сигнатур
WinCVEID	string	Дополнительные параметры событий в windows event log
WinDCDNSName	string	DNS-имя контроллера домена
WinDCOMorRPC	string	Используемый протокол DCOM или RPC
WinDeletedCAPs	string	Список удаленных централизованных политик доступа
WinDestAddress	string	Адрес назначения для сетевого события
WinDestinationDRA	string	Параметры сетевых соединений из событий в windows event log
WinDestPort	string	Порт назначения для сетевого события
WinDetectionID	string	Идентификатор обнаруженной угрозы
WinDetectionSource	string	Источник обнаружения угрозы
WinDetectionSourceIndex	string	Индекс источника обнаружения угрозы
WinDetectionTime	string	Время обнаружения угрозы
WinDetectionType	string	Тип обнаружения угрозы
WinDetectionTypeIndex	string	Индекс типа обнаружения угрозы
WinDetectionUser	string	Пользователь, при котором произошло обнаружение угрозы
WinDeviceClaims	string	Устройства, задействованные в аутентификации
WinDeviceDescription	string	Описание обрабатываемого объекта, указанное в его свойствах
WinDeviceId	string	Идентификатор устройства
WinDirection	string	Направление сетевого трафика
WinDisabledPrivilegeList	string	Список отключенных привилегий
WinDisableIntegrityChecks	string	Флаг отключения проверки целостности
WinDisplayName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinDisposition	string	Результат обработки события или объекта
WinDnsHostName	string	Название устройства пользователя
WinDnsName	string	Название устройства пользователя
WinDomain	string	Домен, связанный с событием или объектом
WinDomainBehaviorVersion	string	Параметры объектов active directory
WinDomainName	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinDomainPolicyChanged	string	Параметры объектов active directory
WinDomainSid	string	Идентификатор безопасности учетной записи (sid)
WinDSName	string	Имя обрабатываемого объекта
WinDSType	string	Тип объекта, обнаруженного по
WinDummy	string	Дополнительные параметры событий в windows event log
WinDuration	string	Продолжительность события
WinDwDataRate	string	Параметры и свойства устройств класса смарт-карта
WinDwDefaultClock	string	Параметры и свойства устройств класса смарт-карта

Поле	Тип	Описание
WinDwFeatures	string	Параметры и свойства устройств класса смарт-карта
WinDwMaxDataRate	string	Параметры и свойства устройств класса смарт-карта
WinDwMaxIFSD	string	Параметры и свойства устройств класса смарт-карта
WinDwMaximumClock	string	Параметры и свойства устройств класса смарт-карта
WinDwMechanical	string	Параметры и свойства устройств класса смарт-карта
WinDwProtocols	string	Параметры и свойства устройств класса смарт-карта
WinDwSyncProtocols	string	Параметры и свойства устройств класса смарт-карта
WinEAPErrorCode	string	Код ошибки EAP
WinEAPReasonCode	string	Код причины ошибки EAP
WinEapRootCauseString	string	Описание основной причины ошибки EAP
WinEAPType	string	Тип EAP-аутентификации
WinEffectiveState	string	Текущее состояние объекта или системы
WinElevatedToken	string	Параметры безопасности из событий в windows event log
WinEnabledPrivilegeList	string	Список включенных привилегий
WinEndUSN	string	Конечный идентификатор изменения в журнале USN
WinEngineVersion	string	Версия движка на момент события
WinEntryType	string	Тип объекта, обнаруженного по
WinErrorCode	string	Параметры операций из событий в windows event log
WinErrorDescription	string	Описание ошибки, возникшей при событии
WinEventCount	string	Количество повторений события
WinEventCountTotal	string	Общее количество связанных событий
WinEventId	string	Идентификатор события
WinEventIdx	string	Индекс события в последовательности
WinEventSourceId	string	Код типа объекта
WinExecutionID	string	Идентификатор процесса, сгенерировавшего событие
WinExecutionName	string	Название процесса, сгенерировавшего событие
WinExecutionStatus	string	Статус выполнения действия
WinExecutionStatusIndex	string	Индекс статуса выполнения действия
WinExeFileName	string	Имя обрабатываемого объекта
WinFailureId	string	Идентификатор ошибки
WinFailurePoint	string	Точка, где произошел сбой
WinFailureReason	string	Причина, по которой файл помещен в категорию
WinFileName	string	Имя обрабатываемого объекта
WinFilterId	string	Идентификатор фильтра
WinFilterKey	string	Ключ фильтра
WinFilterName	string	Название фильтра
WinFilterRTID	string	Параметры сетевых соединений из событий в windows event log
WinFilterType	string	Тип фильтра
WinFlags	string	Параметры операций из событий в windows event log
WinFlightSigning	string	Флаг подписи для тестовых сборок
WinForceLogoff	string	Параметры объектов active directory

Поле	Тип	Описание
WinForestRoot	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinForestRootSid	string	Идентификатор безопасности учетной записи (sid)
WinFQDN	string	Полное доменное имя хоста (FQDN), с которого инициировано событие
WinFullyQualifiedSubjectMachineName	string	Полное имя компьютера субъекта
WinFullyQualifiedSubjectUserName	string	Полное имя пользователя субъекта
WinFWLink	string	Ссылка на страницу с описанием угрозы
WinGPOList	string	Права доступа, которыми обладает обрабатываемый объект
WinGroupDomainName	string	Домен группы
WinGroupMembership	string	Членство в группах
WinGroupName	string	Имя группы
WinGroupPolicyApplied	string	Примененная групповая политика
WinGroupSid	string	SID группы
WinGroupTypeChange	string	Информация о принадлежности пользователя к группе пользователей
WinHandleId	string	Код типа объекта
WinHangType	string	Тип объекта, обнаруженного по
WinHardwareIds	string	Идентификаторы аппаратного обеспечения
WinHomeDirectory	string	Путь к обрабатываемому объекту
WinHomePath	string	Путь к обрабатываемому объекту
WinHypervisorDebug	string	Флаг отладки гипервизора
WinHypervisorLaunchType	string	Тип запуска гипервизора
WinHypervisorLoadOptions	string	Опции загрузки гипервизора
WinIdentity	string	Идентификатор пользователя или устройства
WinImagePath	string	Путь к обрабатываемому объекту
WinImpersonationLevel	string	Параметры безопасности из событий в windows event log
WinInitiatorCookie	string	Файл cookie инициатора операции
WinInterfaceName	string	Имя сетевого интерфейса
WinIntfGuid	string	GUID сетевого интерфейса
WinIpAddress	string	Локальный ip адрес
WinIpAddresses	string	IP-адреса, связанные с объектом
WinIpPort	string	Номера портов источника и получателя обрабатываемого сетевого соединения
WinKerberosPolicyChange	string	Параметры безопасности из событий в windows event log
WinKernelDebug	string	Флаг отладки ядра
WinKeyFilePath	string	Путь к ключевому файлу
WinKeyLength	string	Параметры объектов active directory
WinKeyModName	string	Имя модуля управления ключами
WinKeyName	string	Имя криптографического ключа
WinKeyType	string	Тип криптографического ключа
WinLayerId	string	Идентификатор слоя фильтрации
WinLayerKey	string	Ключ слоя фильтрации
WinLayerName	string	Параметры сетевых соединений из событий в windows event log

Поле	Тип	Описание
WinLayerRTID	string	Параметры сетевых соединений из событий в windows event log
WinLinkName	string	Имя обрабатываемого объекта
WinLmPackageName	string	Имя обрабатываемого объекта
WinLoadOptions	string	Параметры загрузки
WinLocalAddress	string	Локальный адрес в сетевом событии
WinLocalKeyModPort	string	Порт локального модуля ключа
WinLocalMac	string	Локальный MAC-адрес
WinLocalMMPrincipalName	string	Локальный субъект безопасности, который использовался в процессе аутентификации основного режима (IPsec Main Mode)
WinLocationInformation	string	Параметры пользовательских сессий из событий в windows event log
WinLockoutDuration	string	Параметры объектов active directory
WinLockoutObservationWindow	string	Параметры объектов active directory
WinLockoutThreshold	string	Параметры объектов active directory
WinLogDroppedPacketsEnabled	string	Флаг, указывающий включено ли логирование отброшенных сетевых пакетов
WinLoggingResult	string	Результат выполнения логирования
WinLogonGuid	string	Информация о принадлежности пользователя к группе пользователей
WinLogonHours	string	Параметры объектов active directory
WinLogonID	string	Идентификатор безопасности учетной записи (sid)
WinLogonProcessName	string	Имя объекта из события windows event log
WinLogonType	string	Тип сеанса входа в систему
WinLogSuccessfulConnectionsEnabled	string	Флаг, показывающий включено ли логирование успешных сетевых подключений
WinMachineAccountQuota	string	Параметры объектов active directory
WinMachineInventory	string	Инвентаризация машины
WinMajorVersion	string	Версия отправляемой статистики
WinMandatoryLabel	string	Обязательная метка безопасности процесса
WinMasterKeyId	string	Идентификатор основного ключа для шифрования данных
WinMaxPasswordAge	string	Параметры объектов active directory
WinMemberName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinMemberSid	string	Идентификатор безопасности учетной записи (sid)
WinMessageNumber	string	Дополнительные параметры событий в windows event log
WinMessageTotal	string	Дополнительные параметры событий в windows event log
WinMinorVersion	string	Версия отправляемой статистики
WinMinPasswordAge	string	Параметры объектов active directory
WinMinPasswordLength	string	Параметры объектов active directory
WinMixedDomainMode	string	Параметры объектов active directory
WinMMAuthMethod	string	Метод аутентификации, используемый во время согласования основного режима (IPsec Main Mode)
WinMMFilterID	string	Идентификатор, который Windows назначает определенному фильтру основного режима (IPsec Main Mode)
WinMMImpersonationState	string	Поле показывает, использовалось ли имперсонация в процессе аутентификации основного режима (IPsec Main Mode)

Поле	Тип	Описание
WinModifiedCAPs	string	Список модифицированных централизованных политик доступа
WinModifiedObjectProperties	string	Описание обрабатываемого объекта, указанное в его свойствах
WinMulticastFlowsEnabled	string	Флаг включения многоадресных потоков
WinNamingContext	string	Параметры сетевых соединений из событий в windows event log
WinNASIdentifier	string	Идентификатор сетевого доступа (NAS)
WinNASIPv4Address	string	IPv4-адрес сетевого доступа (NAS)
WinNASIPv6Address	string	IPv6-адрес сетевого доступа (NAS)
WinNASPort	string	Порт сетевого доступа, через который проходит соединение
WinNASPortType	string	Тип порта сетевого доступа
WinNetbiosName	string	Имя обрабатываемого объекта
WinNetworkPolicyName	string	Название примененной сетевой политики
WinNewMaxUsers	string	Свойства ресурсов распределённой файловой системы (dfs)
WinNewObjectDN	string	Уникальное имя объекта
WinNewProcessId	string	Идентификатор созданного процесса
WinNewProcessName	string	Имя созданного процесса
WinNewRemark	string	Свойства ресурсов распределённой файловой системы (dfs)
WinNewSd	string	Параметры безопасности из событий в windows event log
WinNewShareFlags	string	Свойства ресурсов распределённой файловой системы (dfs)
WinNewState	string	Новое состояние объекта или системы
WinNewTargetUserName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinNewTime	string	Время события
WinNewUacValue	string	Параметры компонента контроль учетных записей пользователей (uac)
WinNewValue	string	Атрибуты обрабатываемого объекта
WinNewValueType	string	Тип объекта, обнаруженного по
WinNotificationPackageName	string	Имя обрабатываемого объекта
WinObjectClass	string	Битовая маска категорий программ в компоненте обновления программ
WinObjectCollectionName	string	Имя обрабатываемого объекта
WinObjectDN	string	Уникальное имя объекта
WinObjectGUID	string	Информация о принадлежности пользователя к группе пользователей
WinObjectIdentifyingProperties	string	Дополнительные параметры событий в windows event log
WinObjectName	string	Имя объекта из события windows event log
WinObjectProperties	string	Параметры задач, зарегистрированных в событиях в windows event log
WinObjectServer	string	Параметры задач, зарегистрированных в событиях в windows event log
WinObjectType	string	Тип объекта, обнаруженного по
WinObjectValueName	string	Имя обрабатываемого объекта
WinOemInformation	string	Описание обрабатываемого объекта, указанное в его свойствах
WinOldMaxUsers	string	Свойства ресурсов распределённой файловой системы (dfs)
WinOldObjectDN	string	Уникальное имя объекта
WinOldRemark	string	Свойства ресурсов распределённой файловой системы (dfs)
WinOldSd	string	Параметры безопасности из событий в windows event log

Поле	Тип	Описание
WinOldShareFlags	string	Свойства ресурсов распределённой файловой системы (dfs)
WinOldTargetUserName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinOldUacValue	string	Параметры компонента контроль учетных записей пользователей (uac)
WinOldValue	string	Атрибуты обрабатываемого объекта
WinOldValueType	string	Тип объекта, обнаруженного по
WinOpCorrelationID	string	Код типа объекта
WinOperation	string	Тип выполняемой операции
WinOperationId	string	Параметры операций из событий в windows event log
WinOperationMode	string	Режим выполнения операции
WinOperationType	string	Тип объекта, обнаруженного по
WinOptions	string	Параметры операций из событий в windows event log
WinOriginID	string	Идентификатор источника происхождения объекта
WinOriginName	string	Название источника происхождения объекта
WinPackage	string	Имя или идентификатор пакета, связанного с событием
WinPackageFullName	string	Имя обрабатываемого объекта
WinPackageName	string	Имя обрабатываемого объекта
WinPackageRelativeAppId	string	Код типа объекта
WinPackageSid	string	SID пакета, связанного с событием
WinParam1	string	Текст запроса
WinParam2	string	Текст запроса
WinParam3	string	Текст запроса
WinParam4	string	Текст запроса
WinParam5	string	Текст запроса
WinParentProcessId	string	Идентификатор процесса-родителя, который запустил текущий процесс при создании задачи
WinParentProcessName	string	Имя родительского процесса
WinPasswordHistoryLength	string	Параметры объектов active directory
WinPasswordLastSet	string	Параметры объектов active directory
WinPasswordProperties	string	Описание обрабатываемого объекта, указанное в его свойствах
WinPath	string	Путь к обрабатываемому объекту
WinPathFound	string	Путь к обнаруженному файлу или объекту
WinPayload	string	Атрибуты обрабатываемого объекта
WinPeerMac	string	MAC-адрес удаленного устройства
WinPostCleanStatus	string	Статус после очистки угрозы
WinPreAuthType	string	Тип объекта, обнаруженного по
WinPreExecutionStatus	string	Статус до выполнения действия
WinPreviousEngineVersion	string	Предыдущая версия движка защиты
WinPreviousSignatureVersion	string	Предыдущая версия сигнатур
WinPreviousTime	string	Время события
WinPrimaryGroupId	string	Информация о принадлежности пользователя к группе пользователей
WinPrivilegeList	string	Права доступа, которыми обладает обрабатываемый объект

Поле	Тип	Описание
WinProcessCreationTime	string	Время создания процесса
WinProcessId	string	Идентификатор процесса в системе (pid)
WinProcessName	string	Имя обрабатываемого объекта
WinProductName	string	Название продукта безопасности, сгенерировавшего событие
WinProductVersion	string	Версия продукта безопасности
WinProfile	string	Имя или идентификатор профиля пользователя или системы
WinProfileChanged	string	Параметры операций из событий в windows event log
WinProfilePath	string	Путь к обрабатываемому объекту
WinProfiles	string	Список примененных профилей
WinProfileUsed	string	Используемый профиль в событии
WinProperties	string	Описание обрабатываемого объекта, указанное в его свойствах
WinPropertyName	string	Название свойства объекта
WinProtocol	string	Параметры сетевых соединений из событий в windows event log
WinProviderKey	string	Ключ поставщика для фильтра или операции
WinProviderName	string	Имя поставщика для операции или события
WinProxyPolicyName	string	Название политики прокси
WinPuaCount	string	Дополнительные параметры событий в windows event log
WinPuaPolicyId	string	Код типа объекта
WinQfeVersion	string	Версия отправляемой статистики
WinQuarantineSessionIdentifier	string	Идентификатор сессии карантина
WinQuarantineState	string	Состояние объекта в карантине
WinReadOperation	string	Флаг выполнения операции чтения
WinReason	string	Причина события или действия
WinReasonCode	string	Код причины события
WinReasonForRejection	string	Причина отклонения операции
WinReasonText	string	Текстовое описание причины события
WinRecoveryKeyId	string	Идентификатор ключа восстановления
WinRecoveryReason	string	Причина использования ключа восстановления
WinRecoveryServer	string	Сервер восстановления данных
WinRelativeTargetName	string	Имя обрабатываемого объекта
WinRemediationUser	string	Пользователь, инициировавший очистку
WinRemoteAddress	string	Удаленный адрес подключения или операции
WinRemoteAdminEnabled	string	Флаг разрешения удаленного администрирования
WinRemoteEventLogging	string	Флаг удаленного ведения журнала событий
WinRemoteKeyModPort	string	Удаленный порт модуля ключа
WinRemoteMachineID	string	Идентификатор удаленной машины
WinRemoteMMPrincipalName	string	Удаленный субъект безопасности, который использовался в процессе аутентификации основного режима (IPsec Main Mode)
WinRemoteUserID	string	Идентификатор удаленного пользователя
WinReplicationEvent	string	Флаг события репликации
WinReportId	string	Код типа объекта

Поле	Тип	Описание
WinRequestClientInfo	string	Информация о клиенте, отправившем запрос
WinRequestCSPProvider	string	Поставщик CSP, запрошенный в событии
WinRequester	string	Субъект, инициировавший запрос
WinRequestId	string	Идентификатор запроса
WinRequestOSVersion	string	Версия ОС клиента запроса
WinResource	string	Объект или ресурс, над которым выполняется операция
WinResourceAttributes	string	Атрибуты обрабатываемого объекта
WinResourceManager	string	Менеджер ресурса, ответственный за объект
WinResponderCookie	string	Файл cookie ответчика операции
WinRestrictedAdminMode	string	Параметры безопасности из событий в windows event log
WinRestrictedSidCount	string	Количество ограниченных SID для операции
WinReturnCode	string	Код возврата результата операции
WinRole	string	Роль субъекта в операции
WinRpcCallClientLocality	string	Местоположение клиента RPC, инициировавшего событие, указывающее на локальный или удаленный вызов
WinRuleAttr	string	Атрибут правила безопасности или фильтра
WinRuleId	string	Код типа объекта
WinRuleName	string	Имя обрабатываемого объекта
WinRunspaceId	string	Идентификатор рабочего пространства PowerShell
WinSamAccountName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinScanID	string	Идентификатор сканирования
WinScanParameters	string	Параметры сканирования
WinScanParametersIndex	string	Индекс параметров сканирования
WinScanResources	string	Ресурсы, которые были просканированы
WinScanTimeHours	string	Часы, затраченные на сканирование
WinScanTimeMinutes	string	Минуты, затраченные на сканирование
WinScanTimeSeconds	string	Секунды, затраченные на сканирование
WinScanType	string	Тип сканирования
WinScanTypeIndex	string	Индекс типа сканирования
WinSchema	string	Схема объекта или события
WinSchemaFriendlyName	string	Читаемое имя схемы
WinScriptBlockId	string	Код типа объекта
WinScriptBlockText	string	Параметры пользовательских сессий из событий в windows event log
WinScriptPath	string	Путь к обрабатываемому объекту
WinSecurityDescriptor	string	Дескриптор безопасности объекта
WinSecurityPackageName	string	Имя обрабатываемого объекта
WinSerialNumber	string	Серийный номер сертификата или объекта безопасности
WinServerNames	string	Список имён серверов, участвующих в операции
WinService	string	Имя службы или сервисного компонента, связанного с событием
WinServiceAccount	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс

Поле	Тип	Описание
WinServiceFileName	string	Имя обрабатываемого объекта
WinServiceName	string	Имя объекта из события windows event log
WinServicePrincipalNames	string	Имя обрабатываемого объекта
WinServiceSid	string	Идентификатор безопасности учетной записи (sid)
WinServiceStartType	string	Тип запуска службы windows
WinServiceType	string	Тип объекта, обнаруженного по
WinServiceVersion	string	Версия отправляемой статистики
WinSessionId	string	Уникальный идентификатор сеанса входа
WinSessionName	string	Параметры пользовательских сессий из событий в windows event log
WinSettingType	string	Тип объекта, обнаруженного по
WinSettingValue	string	Атрибуты обрабатываемого объекта
WinSeverityID	string	Идентификатор уровня опасности угрозы
WinSeverityName	string	Название уровня опасности угрозы
WinShareLocalPath	string	Путь к обрабатываемому объекту
WinShareName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinSID	string	Идентификатор безопасности (SID), относящийся к пользователю или объекту
WinSidFilteringEnabled	string	Параметры безопасности из событий в windows event log
WinSidHistory	string	Идентификатор безопасности учетной записи (sid)
WinSidList	string	Идентификатор безопасности учетной записи (sid)
WinSignatureType	string	Тип сигнатуры угрозы
WinSignatureTypeIndex	string	Индекс типа сигнатуры угрозы
WinSignatureVersion	string	Версия сигнатуры на момент события
WinSourceAddr	string	Параметры сетевых соединений из событий в windows event log
WinSourceAddress	string	Локальный ip адрес
WinSourceDRA	string	Параметры сетевых соединений из событий в windows event log
WinSourceHandleId	string	Идентификатор дескриптора исходного объекта
WinSourceID	string	Идентификатор источника события или действия
WinSourceName	string	Название источника события или действия
WinSourcePort	string	Номера портов источника и получателя обрабатываемого сетевого соединения
WinSourceProcessId	string	Идентификатор процесса-источника
WinSourceSid	string	SID субъекта, инициировавшего операцию
WinSourceUserName	string	Имя пользователя-источника
WinSpnName	string	Имя SPN (Service Principal Name), используемое для аутентификации
WinSSID	string	Идентификатор беспроводной сети (SSID)
WinStagingReason	string	Причина направления объекта на аудит
WinStartTime	string	Время события
WinStartType	string	Тип объекта, обнаруженного по
WinStartUSN	string	Параметры сетевых соединений из событий в windows event log
WinState	string	Состояние объекта или системы на момент события

Поле	Тип	Описание
WinStatus	string	Описание обрабатываемого объекта, указанное в его свойствах
WinStatusCode	string	Параметры операций из событий в windows event log
WinStatusDescription	string	Описание текущего статуса события или действия
WinStopTime	string	Время события
WinSubcategoryGuid	string	Информация о принадлежности пользователя к группе пользователей
WinSubcategoryId	string	Код типа объекта
WinSubject	string	Информация о субъекте, инициировавшем действие
WinSubjectAlternativeName	string	Поле SAN сертификата, содержащее альтернативные имена субъекта
WinSubjectDomainName	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinSubjectKeyIdentifier	string	Идентификатор ключа субъекта сертификата
WinSubjectLogonId	string	Идентификатор безопасности учетной записи (sid)
WinSubjectMachineName	string	Имя машины, от имени которой выполнялось действие
WinSubjectMachineSID	string	SID машины, от имени которой выполнялось действие
WinSubjectUserDomainName	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinSubjectUserName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinSubjectUserSid	string	Идентификатор безопасности учетной записи (sid)
WinSubStatus	string	Параметры операций из событий в windows event log
WinTargetDomainName	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinTargetHandleId	string	Идентификатор дескриптора целевого объекта
WinTargetInfo	string	Описание обрабатываемого объекта, указанное в его свойствах
WinTargetLinkedLogonId	string	Идентификатор безопасности учетной записи (sid)
WinTargetLogonGuid	string	Информация о принадлежности пользователя к группе пользователей
WinTargetLogonId	string	Идентификатор безопасности учетной записи (sid)
WinTargetName	string	Имя целевого объекта или ресурса
WinTargetOutboundDomainName	string	Имя домена, используемого для аутентификации владельца сеанса входа
WinTargetOutboundUserName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinTargetProcessId	string	Идентификатор процесса в системе (pid)
WinTargetProcessName	string	Имя обрабатываемого объекта
WinTargetServer	string	Целевой сервер события
WinTargetServerName	string	Название устройства пользователя
WinTargetSid	string	Идентификатор безопасности учетной записи (sid)
WinTargetState	string	Состояние целевого объекта после операции
WinTargetUserDomain	string	Домен целевого пользователя
WinTargetUserName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinTargetUserSid	string	Идентификатор безопасности учетной записи (sid)
WinTaskContent	string	Исходное содержимое задачи планировщика, связанной с событием
WinTaskContentActionsContext	string	Параметры заданий планировщика задач операционной системы

Поле	Тип	Описание
WinTaskContentActionsExecCommand	string	Аргументы командной строки, переданные процессу при запуске
WinTaskContentPrincipalsPrincipalid	string	Идентификатор безопасности учетной записи (sid)
WinTaskContentPrincipalsPrincipalLogonType	string	Тип сеанса входа в систему
WinTaskContentPrincipalsPrincipalRunLevel	string	Параметры заданий планировщика задач операционной системы
WinTaskContentPrincipalsPrincipalUserId	string	Идентификатор безопасности учетной записи (sid)
WinTaskContentRegistrationInfoAuthor	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinTaskContentRegistrationInfoDate	string	Дата события
WinTaskContentSettingsAllowHardTerminate	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsAllowStartOnDemand	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsDisallowStartIfOnBatteries	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsEnabled	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsExecutionTimeLimit	string	Время события
WinTaskContentSettingsHidden	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsIdleSettingsRestartOnIdle	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsIdleSettingsStopOnIdleEnd	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsMultipleInstancesPolicy	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsPriority	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsRunOnlyIfIdle	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsRunOnlyIfNetworkAvailable	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsStartWhenAvailable	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsStopIfGoingOnBatteries	string	Параметры заданий планировщика задач операционной системы
WinTaskContentSettingsWakeToRun	string	Параметры заданий планировщика задач операционной системы
WinTaskContentTriggers	string	Параметры задач, зарегистрированных в событиях в windows event log
WinTaskContentversion	string	Версия задачи в её исходном содержимом
WinTaskContentNew	string	Изменённое содержимое задачи планировщика
WinTaskContentNewActionsContext	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewActionsExecCommand	string	Аргументы командной строки, переданные процессу при запуске
WinTaskContentNewPrincipalsPrincipalid	string	Идентификатор безопасности учетной записи (sid)
WinTaskContentNewPrincipalsPrincipalLogonType	string	Тип сеанса входа в систему
WinTaskContentNewPrincipalsPrincipalRunLevel	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewPrincipalsPrincipalUserId	string	Идентификатор безопасности учетной записи (sid)
WinTaskContentNewRegistrationInfoAuthor	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinTaskContentNewRegistrationInfoDate	string	Дата события
WinTaskContentNewSettingsAllowHardTerminate	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsAllowStartOnDemand	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsDisallowStartIfOnBatteries	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsEnabled	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsExecutionTimeLimit	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsHidden	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsIdleSettingsRestartOnIdle	string	Параметры заданий планировщика задач операционной системы

Поле	Тип	Описание
WinTaskContentNewSettingsIdleSettingsStopOnIdleEnd	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsMultipleInstancesPolicy	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsPriority	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsRunOnlyIfIdle	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsRunOnlyIfNetworkAvailable	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsStartWhenAvailable	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsStopIfGoingOnBatteries	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewSettingsWakeToRun	string	Параметры заданий планировщика задач операционной системы
WinTaskContentNewTriggers	string	Параметры задач, зарегистрированных в событиях в windows event log
WinTaskContentNewversion	string	Версия задачи в обновлённом содержимом
WinTaskName	string	Имя обрабатываемого объекта
WinTdoAttributes	string	Атрибуты обрабатываемого объекта
WinTdoDirection	string	Параметры сетевых соединений из событий в windows event log
WinTdoType	string	Тип объекта, обнаруженного по
WinTemplateContent	string	Содержимое шаблона сертификата
WinTemplateDSObjectFQDN	string	Полное доменное имя (FQDN) объекта шаблона в каталоге Active Directory
WinTemplateInternalName	string	Внутреннее имя шаблона сертификата
WinTemplateOID	string	Идентификатор объекта шаблона сертификата
WinTemplateSchemaVersion	string	Версия схемы шаблона сертификата
WinTemplateVersion	string	Версия шаблона сертификата
WinTerminationTime	string	Время события
WinTestSigning	string	Флаг, указывающий включён ли режим тестовой подписи в системе
WinThreatID	string	Идентификатор угрозы
WinThreatName	string	Название угрозы
WinTicketEncryptionType	string	Тип объекта, обнаруженного по
WinTicketOptions	string	Параметры объектов active directory
WinTokenElevationType	string	Тип повышения токена безопасности
WinTopLevelName	string	Имя обрабатываемого объекта
WinTransactionId	string	Код типа объекта
WinTransitionsToOn	string	Переход объекта или компонента в состояние «включено»
WinTransmittedServices	string	Параметры операций из событий в windows event log
WinTreeDelete	string	Дополнительные параметры событий в windows event log
WinType	string	Тип события или объекта
WinTypeID	string	Идентификатор типа события или угрозы
WinTypeName	string	Название типа события или угрозы
WinUnused	string	Зарезервированное или неиспользуемое поле
WinUnused2	string	Дополнительное зарезервированное поле, не используемое событием
WinUnused3	string	Дополнительное зарезервированное поле, не используемое событием
WinUnused4	string	Дополнительное зарезервированное поле, не используемое событием
WinUnused5	string	Дополнительное зарезервированное поле, не используемое событием

Поле	Тип	Описание
WinUnused6	string	Дополнительное зарезервированное поле, не используемое событием
WinUpdateType	string	Тип обновления продукта или сигнатуры
WinUpdateTypeIndex	string	Индекс типа обновления продукта или сигнатуры
WinUser	string	Имя пользователя, связанного с событием
WinUserAccountControl	string	Параметры компонента контроль учетных записей пользователей (uac)
WinUserClaims	string	Список заявок пользователя для нового сеанса входа
WinUserData	string	Параметры пользовательских сессий из событий в windows event log
WinUserName	string	Имя пользователя
WinUserParameters	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinUserPrincipalName	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinUserSid	string	SID пользователя, связанного с событием
WinUserUPN	string	User Principal Name (UPN) пользователя
WinUserWorkstations	string	Название устройства пользователя
WinVendorIds	string	Параметры пользовательских сессий из событий в windows event log
WinVirtualAccount	string	Идентификатор учетной записи, от имени которой был запущен контролируемый процесс
WinVsmLaunchType	string	Тип запуска Virtual Secure Mode (VSM)
WinWakeFromState	string	Состояние, из которого система была выведена (сон, гибернация и т.д.)
WinWakeRequesterTypeAc	string	Тип инициатора пробуждения при работе от сети
WinWakeRequesterTypeDc	string	Тип инициатора пробуждения при работе от батареи
WinWeight	string	Вес или приоритет, связанный с объектом события
WinWorkstation	string	Название устройства пользователя
WinWorkstationName	string	Название устройства пользователя
WinProcessingErrorDataDataItemName	string	Имя элемента данных, вызвавшего ошибку обработки
WinProcessingErrorDataErrorCode	string	Код ошибки, возникшей при обработке события
WinProcessingErrorDataEventPayload	string	Исходные данные события, вызвавшие ошибку
WinSystemChannel	string	Канал журнала событий Windows, из которого получено событие
WinSystemComputer	string	Имя компьютера, на котором было сгенерировано событие
WinSystemEventID	string	Идентификатор события, определяющий тип произошедшего события в систем
WinSystemEventIDQualifiers	string	Дополнительные квалификаторы события, предоставляющие расширенную информацию о событии
WinSystemEventRecordID	string	Уникальный идентификатор записи события в журнале
WinSystemExecutionProcessID	string	Идентификатор процесса (PID), связанного с выполнением события
WinSystemExecutionThreadID	string	Идентификатор потока (TID), который вызвал событие
WinSystemKeywords	string	Ключевые слова события, используемые для классификации и фильтрации событий
WinSystemLevel	string	Уровень события, указывающий на его важность или критичность
WinSystemOpcode	string	Код операции события, описывающий тип действия, связанного с событием
WinSystemProviderEventSourceName	string	Имя источника, который сгенерировал событие
WinSystemProviderGuid	string	Глобальный уникальный идентификатор провайдера события

Поле	Тип	Описание
WinSystemProviderName	string	Имя провайдера события
WinSystemSecurityUserID	string	Идентификатор пользователя, связанный с событием
WinSystemTask	string	Идентификатор задачи события
WinSystemTimeCreatedSystemTime	string	Время создания события
WinSystemVersion	string	Версия схемы события
WinAutoBackupBackupPath	string	Путь к файлу или папке, куда выполняется автоматическое резервное копирование
WinAutoBackupChannel	string	Канал или источник, используемый для автоматического резервного копирования
WinEventProcessingFailureErrorCode	string	Код ошибки, возникшей при обработке события
WinEventProcessingFailureEventID	string	ID события, при обработке которого произошла ошибка
WinEventProcessingFailurePublisherID	string	Идентификатор приложения или службы, пытавшейся зарегистрировать событие, вызвавшее ошибку
WinEventXMLAddress	string	Адрес, связанный с событием
WinEventXMLParam1	string	Поле дополнительной информации о событии
WinEventXMLParam2	string	Поле дополнительной информации о событии
WinEventXMLParam3	string	Поле дополнительной информации о событии
WinEventXMLSessionID	string	Идентификатор сессии пользователя, связанной с событием
WinEventXMLSource	string	Источник события
WinEventXMLTargetSession	string	Целевая сессия, к которой относится событие
WinEventXMLUser	string	Пользователь, связанный с событием
WinFileIsFull	string	Индикатор того, что журнал заполнен и больше не может принимать новые записи
WinLogFileClearedSubjectDomainName	string	Домен пользователя, который очистил журнал событий
WinLogFileClearedSubjectLogonId	string	Идентификатор входа пользователя, который очистил журнал событий
WinLogFileClearedSubjectUserName	string	Имя пользователя, который очистил журнал событий
WinLogFileClearedSubjectUserSid	string	SID пользователя, который очистил журнал событий
WinOperationClientFailureClientMachine	string	Имя компьютера клиента, на котором произошла ошибка операции
WinOperationClientFailureClientProcessId	string	Идентификатор процесса клиента, вызвавшего сбой операции
WinOperationClientFailureComponent	string	Компонент системы, в котором произошла ошибка операции
WinOperationClientFailureId	string	Уникальный идентификатор ошибки операции
WinOperationClientFailureOperation	string	Название или описание операции, которая завершилась сбоем
WinOperationClientFailurePossibleCause	string	Возможная причина сбоя операции
WinOperationClientFailureResultCode	string	Код результата операции, указывающий на успешность или причину сбоя
WinOperationClientFailureUser	string	Пользователь, инициировавший операцию, которая завершилась сбоем
WinOperationStartedOperationalCode	string	Код начатой операции
WinOperationStartedOperationalHostProcess	string	Процесс хоста, инициировавший операцию
WinOperationStartedOperationalProcessID	string	Идентификатор процесса, связанного с начатой операцией
WinOperationStartedOperationalProviderName	string	Имя провайдера или источника события
WinOperationStartedOperationalProviderPath	string	Путь к провайдеру или источнику события
WinServiceShutdown	string	Служба Windows была остановлена

Blocked Document

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Blocked Document

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса

Поле	Тип	Описание
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS

Поле	Тип	Описание
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS

Поле	Тип	Описание
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Applock

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса

Поле	Тип	Описание
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessCalltrace	string	Трассировка стека функций вызова процесса
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла

Поле	Тип	Описание
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS

Поле	Тип	Описание
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса

Поле	Тип	Описание
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Process Terminated

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Process Terminated

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessCalltrace	string	Трассировка стека функций вызова процесса
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла

Поле	Тип	Описание
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd

Поле	Тип	Описание
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)

Поле	Тип	Описание
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
ProcessTerminationtime	int	Время, когда процесс был завершён

Device

Этот тип событий поддерживается в операционных системах Windows.

Поля события Device

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventVersion	string	
EventType	string	Тип события
EventId	string	Уникальный идентификатор события

Поле	Тип	Описание
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
DeviceId	string	Идентификатор устройства
DeviceName	string	Имя устройства
DevicePath	string	Путь к устройству
DeviceOperationtype	string	Тип действия устройства
DeviceType	string	Тип устройства
DeviceSystemflag	string	Флаг, если устройство является системным

File System Mount

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события File System Mount

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки

Поле	Тип	Описание
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
VolumeName	string	Системное имя тома
VolumePath	string	Путь, по которому произошло монтирование (точка монтирования)
DeviceClass	string	GUID класса устройства
DeviceId	string	Предоставляемая системой строка, уникальным образом идентифицирующая подключаемое устройство в системе
DeviceBustype	string	Тип шины подключенного устройства
DeviceType	string	Признак, является ли устройство извлекаемым: "removable" - является / "not removable" - не является
DeviceHotpluggable	string	Флаг поддержки горячего подключения: "true" - поддерживает / "false" - не поддерживает
DeviceSerialnumber	string	Серийный номер подключенного устройства
VolumeFilesystemtype	string	Тип файловой системы
DeviceSpaceTotal	uint	Общий объем диска (в МБ)
DeviceSpaceUsed	uint	Использованное место на диске (в МБ)
DeviceSpaceFree	uint	Доступное свободное место на диске (в МБ)

File System Unmount

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события File System Unmount

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
VolumeName	string	Системное имя тома
VolumePath	string	Путь, по которому произошло монтирование (точка монтирования)
DeviceClass	string	GUID класса устройства
DeviceId	string	Предоставляемая системой строка, уникальным образом идентифицирующая подключаемое устройство в системе
DeviceBustype	string	Тип шины подключенного устройства
DeviceType	string	Признак, является ли устройство извлекаемым: "removable" - является / "not removable" - не является
DeviceHotpluggable	string	Флаг поддержки горячего подключения: "true" - поддерживает / "false" - не поддерживает
DeviceSerialnumber	string	Серийный номер подключенного устройства
VolumeFilesystemtype	string	Тип файловой системы
DeviceSpaceTotal	uint	Общий объем диска (в МБ)
DeviceSpaceUsed	uint	Использованное место на диске (в МБ)
DeviceSpaceFree	uint	Доступное свободное место на диске (в МБ)

Bits Job Create

Этот тип событий поддерживается в операционных системах Windows.

Поля события Bits Job Create

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)

Поле	Тип	Описание
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobOwnerUserName	string	Имя владельца задачи
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полный путь к файлу исполняемого процесса
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса

Поле	Тип	Описание
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип исполняемого файла процесса
ProcessFileUrl	string	URL, с которого был загружен исполняемый файла процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса

Поле	Тип	Описание
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла
ParentProcessFileSignSubjectname	string	Имя субъекта сертификата, которым был подписан файл
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Список флагов прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен прародительский процесс
GrandParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла прародительского процесса
GrandParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла)
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл прародительского процесса
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время, когда файл был подписан
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса

Поле	Тип	Описание
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Bits Job Complete

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobOwnerUserName	string	Имя владельца задачи
BitsjobUserName	string	Пользователь, от имени которого выполняется операция

Поле	Тип	Описание
BitsjobFilestotal	int	Число переданных файлов
BitsjobBytestransferred	int	Объем переданных данных
BitsjobPeerBytestransferred	int	Объем переданных данных с использованием p2p

Bits Job Start

Этот тип событий поддерживается в операционных системах Windows.

Поля события Bits Job Start

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие

Поле	Тип	Описание
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobTransferid	string	Уникальный идентификатор передачи guid (файла в задаче)
BitsjobRemotename	string	Url источника данных
BitsjobDatasourceCreationtime	int	Время создания источника данных
BitsjobDatasourceSize	int	Размер источника данных
BitsjobBytestotal	int	Общий обем данных в задаче
BitsjobBytestransferred	int	Объем переданных данных
BitsjobPeerHostname	int	Имя источника данных в p2p
BitsjobPeerBytestransferred	int	Объем переданных данных с использованием p2p

Bits Job Stop

Этот тип событий поддерживается в операционных системах Windows.

Поля события Bits Job Stop

Поле	Тип	Описание
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)

Поле	Тип	Описание
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobTransferid	string	Уникальный идентификатор передачи guid (файла в задаче)
BitsjobRemotename	string	URL источника данных
BitsjobDatasourceCreationtime	int	Время создания источника данных
BitsjobDatasourceSize	int	Размер источника данных
BitsjobBytestotal	int	Общий объем переданных данных
BitsjobBytestransferred	int	Объем переданных данных
BitsjobResultStatuscode	int	Результат выполнения операции по передаче данных через BITS
BitsjobResultAdditionalinfo	int	Дополнительная информация по результату выполнения операции передачи данных через BITS
BitsjobPeerHostname	string	Имя источника данных в p2p
BitsjobPeerContextinfo	int	Идентификатор/параметры источника данных P2P
BitsjobPeerProtocolflags	int	Конфигурация флагов, определяющая возможность передачи или получения данных по p2p
BitsjobPeerBytestransferred	int	Объем переданных данных с использованием p2p
BitsjobProxy	string	Используемый при передаче данных прокси сервер
BitsjobBandwidthLimit	int	Максимальная скорость, которую задание BITS может использовать для загрузки или выгрузки данных
BitsjobBandwidthIgnoreonlan	int	Параметр определяет, нужно ли игнорировать ограничения скорости, если источник или получатель находится в локальной сети

Bits Job Add File

Этот тип событий поддерживается в операционных системах Windows.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobOwnerUserName	string	Имя владельца задачи
BitsjobUserName	string	Пользователь, от имени которого выполняется операция

Поле	Тип	Описание
BitsjobFilestotal	int	Общее число файлов в задаче
BitsjobRemotename	string	URL источника данных
BitsjobLocalname	string	Путь к файлу для сохранения данных
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс

Поле	Тип	Описание
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса

Поле	Тип	Описание
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Bits Job Error

Этот тип событий поддерживается в операционных системах Windows.

Поля события Bits Job Error

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
BitsjobErrorid	int	Идентификатор ошибки
BitsjobId	string	Уникальный идентификатор задачи (guid)
BitsjobName	string	Отображаемое имя задачи
BitsjobTransferid	string	Уникальный идентификатор передачи файла в задаче (GUID)
BitsjobRemotename	string	URL источника данных
BitsjobDatasourceCreationtime	int	Время создания источника данных
BitsjobDatasourceSize	int	Размер источника данных
BitsjobBytestotal	int	Общий объем данных в задаче
BitsjobBytestransferred	int	Объем переданных данных в байтах
BitsjobResultStatuscode	int	Результат выполнения операции по передаче данных через BITS
BitsjobResultAdditionalinfo	int	Дополнительная информация по результату выполнения операции передачи данных через BITS
BitsjobPeerHostname	string	Имя источника данных в p2p

Поле	Тип	Описание
BitsjobPeerContextinfo	int	Идентификатор/параметры источника данных P2P
BitsjobPeerProtocolflags	int	Конфигурация флагов, определяющая возможность передачи или получения данных по p2p
BitsjobPeerBytestransferred	int	Объем переданных данных с использованием p2p
BitsjobProxy	string	Используемый при передаче данных прокси сервер
BitsjobBandwidthLimit	int	Максимальная скорость, которую задание BITS может использовать для загрузки или выгрузки данных
BitsjobBandwidthIgnoreonlan	uint	Параметр определяет, нужно ли игнорировать ограничения скорости, если источник или получатель находится в локальной сети
BitsjobOwnerUserName	string	Имя владельца задачи

Service Create

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Service Create

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении

Поле	Тип	Описание
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
ServiceTitle	string	Имя сервиса, уникальный идентификатор сервиса
ServiceType	string	Тип сервиса
ServiceStarttype	string	Тип запуска сервиса
ServiceCmdline	string	Командная строка запускаемого сервиса
ServiceLoadordergroup	string	Имя группы упорядочения загрузки, к которой принадлежит эта служба
ServiceTagid	uint	Уникальное значение тега для этой службы в группе ServiceLoadOrderGroup
ServiceDependencies	string	Имена сервисов или групп упорядочивания загрузки, которые должны начинаться перед этим сервисом
ServiceStartname	string	Имя учетной записи от которой будет запускаться сервис
ServiceDisplayname	string	Отображаемое имя сервиса
ServiceDeletedelayed	uint	Флаг отложенного удаления. 1 - сервис будет удален, когда остановится; 0 - сервис удален сразу. Для "Service Create" данное поле опционально
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса

Поле	Тип	Описание
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс

Service Modify

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Service Modify

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2

Поле	Тип	Описание
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
ServiceTitle	string	Имя сервиса, уникальный идентификатор сервиса
ServiceType	string	Тип сервиса
ServiceStarttype	string	Тип запуска сервиса
ServiceCmdline	string	Командная строка запускаемого сервиса
ServiceLoadordergroup	string	Имя группы упорядочения загрузки, к которой принадлежит эта служба
ServiceTagid	uint	Уникальное значение тега для этой службы в группе ServiceLoadOrderGroup
ServiceDependencies	string	Имена сервисов или групп упорядочивания загрузки, которые должны начинаться перед этим сервисом
ServiceStartname	string	Имя учетной записи от которой будет запускаться сервис
ServiceDisplayname	string	Отображаемое имя сервиса
ServiceOldType	string	Тип сервиса до изменения
ServiceOldStarttype	string	Тип запуска сервиса до изменения
ServiceOldCmdline	string	Путь до исполняемого файла до изменения
ServiceOldLoadordergroup	string	Имя группы упорядочения загрузки, к которой принадлежит эта служба до изменения
ServiceOldTagid	uint	Уникальное значение тега для этой службы в группе ServiceLoadOrderGroup до изменения
ServiceOldDependencies	string	Имена сервисов или групп упорядочивания загрузки, которые должны начинаться перед этим сервисом до изменения
ServiceOldStartname	string	Имя учетной записи от которой будет запускаться сервис до изменения
ServiceOldDisplayname	string	Отображаемое имя сервиса до изменения
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessIntegritylevel	int	Уровень целостности процесса

Поле	Тип	Описание
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс

Service Delete

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла

Поле	Тип	Описание
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileType	string	Тип файла
FileAttr	int	Атрибуты файловой системы
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
ServiceTitle	string	Имя сервиса, уникальный идентификатор сервиса
ServiceType	string	Тип сервиса
ServiceStarttype	string	Тип запуска сервиса
ServiceCmdline	string	Командная строка запускаемого сервиса
ServiceLoadordergroup	string	Имя группы упорядочения загрузки, к которой принадлежит эта служба
ServiceTagid	uint	Уникальное значение тега для этой службы в группе ServiceLoadOrderGroup
ServiceDependencies	string	Имена сервисов или групп упорядочивания загрузки, которые должны начинаться перед этим сервисом
ServiceStartname	string	Имя учетной записи от которой будет запускаться сервис
ServiceDisplayname	string	Отображаемое имя сервиса
ServiceDeletedelayed	uint	Флаг отложенного удаления. 1 - сервис будет удален, когда остановится; 0 - сервис удален сразу. Для "Service Create" данное поле опционально
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса

Поле	Тип	Описание
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс

Scheduled Task Create

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Scheduled Task Create

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки

Поле	Тип	Описание
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
TaskName	string	Имя задачи, уникальный идентификатор сервиса.
TaskAuthorName	string	Имя пользователя, создавшего задачу
TaskUserName	string	Имя пользователя, от имени которого будет запущена задача
TaskUserId	int	ID пользователя, от имени которого будет запущена задача. Только для Linux/Mac OC
TaskUserSid	string	SID пользователя, от имени которого будет запущена задача. Только для Windows
TaskRunlevel	string	Уровень привилегий, с которыми запускается задача
TaskCreationtime	int	Дата создания задачи
TaskCmdline	string	Действия, выполняемые задачей
TaskEnabled	string	Флаг включена ли задача
TaskHidden	string	Флаг является ли задача скрытой
TaskLocation	string	Путь до объекта задачи в операционной системе
TaskSchedule	string	Расписание запуска задачи
TaskSource	string	Источник задачи
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса

Поле	Тип	Описание
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла

Поле	Тип	Описание
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS

Поле	Тип	Описание
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс

Поле	Тип	Описание
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета

Поле	Тип	Описание
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Scheduled Task Modify

Этот тип событий поддерживается в операционных системах Windows (Windows Vista, Windows Server 2008 и более поздние версии) и Linux.

Поля события Scheduled Task Modify

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки

Поле	Тип	Описание
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
TaskName	string	Имя задачи, уникальный идентификатор сервиса.
TaskAuthorName	string	Имя пользователя, создавшего задачу
TaskUserName	string	Имя пользователя, от имени которого будет запущена задача
TaskUserSid	string	SID пользователя, от имени которого будет запущена задача. Только для Windows
TaskRunlevel	string	Уровень привилегий, с которыми запускается задача
TaskCreationtime	int	Дата создания задачи
TaskCmdline	string	Действия, выполняемые задачей
TaskEnabled	string	Флаг включена ли задача
TaskHidden	string	Флаг является ли задача скрытой
TaskLocation	string	Путь до объекта задачи в операционной системе
TaskSchedule	string	Расписание запуска задачи
TaskSource	string	Источник задачи
TaskOldUserName	string	Предыдущее имя пользователя, от которого запускалась задача
TaskOldUserSid	string	SID предыдущего пользователя, от имени которого будет запущена задача
TaskOldEnabled	string	Предыдущее значение флага включена ли задача
TaskOldHidden	string	Предыдущее значение флага является ли задача скрытой

Поле	Тип	Описание
TaskOldRunlevel	string	Предыдущий уровень привилегий, с которыми запускается задача
TaskOldCmdline	string	Предыдущие действия, выполняемые задачей
TaskOldSchedule	string	Предыдущее расписание запуска задачи
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс

Поле	Тип	Описание
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса

Поле	Тип	Описание
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Scheduled Task Delete

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Scheduled Task Delete

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
TaskName	string	Имя задачи, уникальный идентификатор сервиса.
TaskAuthorName	string	Имя пользователя, создавшего задачу
TaskUserName	string	Имя пользователя, от имени которого будет запущена задача
TaskUserId	int	ID пользователя, от имени которого будет запущена задача. Только для Linux/Mac OC
TaskUserSid	string	SID пользователя, от имени которого будет запущена задача. Только для Windows
TaskRunlevel	string	Уровень привилегий, с которыми запускается задача
TaskCreationtime	int	Дата создания задачи
TaskCmdline	string	Действия, выполняемые задачей
TaskEnabled	string	Флаг включена ли задача
TaskHidden	string	Флаг является ли задача скрытой
TaskLocation	string	Путь до объекта задачи в операционной системе
TaskSchedule	string	Расписание запуска задачи

Поле	Тип	Описание
TaskSource	string	Источник задачи
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса

Поле	Тип	Описание
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса

Поле	Тип	Описание
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false

Поле	Тип	Описание
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File Owner Change

Этот тип событий поддерживается в операционных системах Windows и Linux за исключением Windows XP x64, Windows Server 2003 x64 и Linux с версией ядра более ранней, чем 4.19.*.

Поля события File Owner Change

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки

Поле	Тип	Описание
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileOldOwnerUserName	string	Имя учетной записи в домене предыдущего владельца файла
FileOldOwnerGroupName	string	Имя доменной группы предыдущего владельца файла
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла

Поле	Тип	Описание
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла

Поле	Тип	Описание
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса

Поле	Тип	Описание
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

File ACL Change

Этот тип событий поддерживается в операционных системах Windows и Linux за исключением Windows XP x64, Windows Server 2003 x64 и Linux с версией ядра более ранней, чем 4.19.*.

Поля события File ACL Change

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост

Поле	Тип	Описание
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
FileDacl	string	Список записей управления доступом, определенных в DACL файла
FileOldDacl	string	Предыдущий список записей управления доступом, определенных в DACL файла
FileModifiedDacl	string	Список изменившихся записей из DACL файла
FileSacl	string	Список записей управления доступом, определенных в SACL файла
FileOldSacl	string	Предыдущий список записей управления доступом, определенных в SACL файла
FileModifiedSacl	string	Список изменившихся записей из SACL файла
FileName	string	Имя файла (без пути)
FilePath	string	Полный путь к файлу (без имени файла)
FileFullname	string	Полный путь к файлу
FileMd5	string	MD5-хэш файла
FileSha256	string	SHA256 хэш содержимого файла
FileSize	int	Размер файла в байтах
FileCreationtime	int	Время создания файла
FileModificationtime	int	Время последнего изменения файла
FileOwnerUserId	int	Идентификатор пользователя - владельца файла. Указывается для Linux и macOS
FileOwnerUserName	string	Имя пользователя владельца файла. Указывается для Linux и macOS
FileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла. Указано для Linux и macOS
FileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла. Указывается для Linux и macOS
FileType	string	Тип файла
FileCapPermitted	string	Набор разрешённых возможностей файла
FileCapInheritable	string	Наследуемые возможности файла
FileCapEffective	string	Эффективные возможности файла
FileOpenflags	string	Указанные флаги открытия (например, O_RDWR | O_APPEND), для операций создания/изменения/чтения.
FileAttrModificationtime	int	Последнее время, когда атрибуты файла были изменены
FileAttr	int	Атрибуты файловой системы
FileZoneidentifier	int	Идентификатор зоны, полученный из альтернативного потока "Zone.identifier"
FileProductname	string	Значение имени продукта из ресурса VERSIONINFO файла
FileProductvendor	string	Значение имени компании из ресурса VERSIONINFO файла
FileDescription	string	Описание из ресурса VERSIONINFO файла
FileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO файла
FileSignSubjectname	string	Информация об организации, подписавшей файл

Поле	Тип	Описание
FileSignResult	string	Результат проверки подписи файла: пройдена - true, иначе - false
FileSignTimestamp	int	Дата и время подписания файла
FileUrl	string	URL, с которого был скачан файл
FileEmailSrcAddress	string	Адрес отправителя, с которого файл был получен как вложение
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса

Поле	Тип	Описание
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса

Поле	Тип	Описание
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен

Поле	Тип	Описание
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry Owner Change

Этот тип событий поддерживается в операционных системах Windows за исключением Windows XP x64 и Windows Server 2003 x64.

Поля события Registry Owner Change

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были застронуты событием
RegOwnerUserName	string	Имя учетной записи в домене владельца ключа реестра
RegOldOwnerUserName	string	Имя учетной записи в домене предыдущего владельца ключа реестра
RegOwnerGroupName	string	Имя доменной группы владельца ключа реестра
RegOldOwnerGroupName	string	Имя доменной группы предыдущего владельца ключа реестра

Поле	Тип	Описание
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).

Поле	Тип	Описание
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Registry ACL Change

Этот тип событий поддерживается в операционных системах Windows за исключением Windows XP x64 и Windows Server 2003 x64.

Поля события Registry ACL Change

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки

Поле	Тип	Описание
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
RegKeyName	string	Полный путь и имя ключа реестра, которые были застронуты событием
RegDacl	string	Список записей управления доступом, определенных в DACL ключа реестра
RegOldDacl	string	Предыдущий список записей управления доступом, определенных в DACL ключа реестра
RegModifiedDacl	string	Список изменившихся записей из DACL ключа реестра
RegSacl	string	Набор записей управления доступом в SACL ключа реестра
RegOldSacl	string	Предыдущий список записей управления доступом, определенных в SACL ключа реестра
RegModifiedSacl	string	Список изменившихся записей из SACL ключа реестра
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса

Поле	Тип	Описание
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс

Поле	Тип	Описание
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса

Поле	Тип	Описание
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Executable Memory Mapped

Этот тип событий поддерживается в операционных системах Linux.

Поля события Executable Memory Mapped

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки

Поле	Тип	Описание
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
SyscallArgs	string	Аргументы системных вызовов
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданного процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS

Поле	Тип	Описание
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла

Поле	Тип	Описание
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	string	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен

Поле	Тип	Описание
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса

Поле	Тип	Описание
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	string	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Agent Start

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Agent Start

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)

Поле	Тип	Описание
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
InitiatorId	string	Идентификатор инициатора события
InitiatorName	string	Имя инициатора события
InitiatorType	string	Тип инициатора события
AgentInstanceid	string	Идентификатор уникального запуска агента
ProcessId	int	Идентификатор процесса
ProcessUniqueid	int	Уникальный идентификатор процесса

Agent Stop

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Agent Stop

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Время, когда событие сгененировано агентом (когда событие произошло на хосте)

Поле	Тип	Описание
EventReceivedtimestamp	int	Время, когда сервер принял событие.
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя защищаемого хоста
HostIp	string	IP-адрес защищаемого хоста
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Дата и время выпуска KDB-баз, используемых агентом
AgentSw2Timestamp	int	Дата и время выпуска BSS-баз, используемых агентом
AgentIndexTimestamp	int	Дата и время последнего обновления баз всех компонентов
InitiatorId	string	Идентификатор инициатора события
InitiatorName	string	Имя инициатора события
InitiatorType	string	Тип инициатора события
AgentInstanceid	string	Идентификатор уникального запуска агента
ProcessId	int	Системный идентификатор процесса агента
ProcessUniqueid	int	Уникальный идентификатор процесса агента
AgentStopreason	string	Причина завершения агента: NormalExit - в случае нормальной остановки, exit code = 0. Crash - в случае завершения приложения по сигналу. Freeze - продукт завис. Может дополнительно в себе содержать: ExceedeMemoryLimit - превышен лимит потребления памяти; GenericFailure - в случае остановок приложения со всеми != 0 кодами возврата; Unknown - во всех остальных случаях.
AgentExitcode	int	Код завершения процесса агента

Agent Install

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Agent Install

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий

Поле	Тип	Описание
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
InitiatorId	string	Идентификатор инициатора события
InitiatorName	string	Имя инициатора события
InitiatorType	string	Тип инициатора события

Agent Uninstall

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события Agent Uninstall

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки

Поле	Тип	Описание
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Время, когда событие сгененировано агентом (когда событие произошло на хосте)
EventReceivedtimestamp	int	Время, когда сервер принял событие.
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя защищаемого хоста
HostIp	string	IP-адрес защищаемого хоста
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Дата и время выпуска KDB-баз, используемых агентом
AgentSw2Timestamp	int	Дата и время выпуска BSS-баз, используемых агентом
AgentIndexTimestamp	int	Дата и время последнего обновления баз всех компонентов
InitiatorId	string	Идентификатор инициатора события
InitiatorName	string	Имя инициатора события
InitiatorType	string	Тип инициатора события

Agent Action

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Время, когда событие сгененировано агентом (когда событие произошло на хосте)
EventReceivedtimestamp	int	Время, когда сервер принял событие.
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя защищаемого хоста
HostIp	string	IP-адрес защищаемого хоста
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Дата и время выпуска KDB-баз, используемых агентом
AgentSw2Timestamp	int	Дата и время выпуска BSS-баз, используемых агентом
AgentIndexTimestamp	int	Дата и время последнего обновления баз всех компонентов
InitiatorId	string	Идентификатор инициатора события
InitiatorName	string	Имя инициатора события
InitiatorType	string	Тип инициатора события
AgentInstanceid	string	Идентификатор уникального запуска агента
ProcessId	int	Системный идентификатор процесса агента

Поле	Тип	Описание
ProcessUniqueid	int	Уникальный идентификатор процесса агента
AgentActionType	string	Тип действия в агенте: 0 → SelfProtectionDisabled,1 → SelfProtectionEnabled,2 → SelfProtectionTriggered,3 → PasswordProtectionOn,4 → PasswordProtectionOff,5 → CheckedPermission,В остальных случаях → Unknown
AgentActionDescription	string	Описание действия в агенте
AgentResultcode	int	Код результата действия в агенте

System Startup

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события System Startup

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста

Поле	Тип	Описание
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов

System Shutdown

Этот тип событий поддерживается в операционных системах Windows, Linux и macOS.

Поля события System Shutdown

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост

Поле	Тип	Описание
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux, macOS)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Версия продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов

Connection Close

Включение события `Connection Close` может привести к значительному увеличению потребления ресурсов на защищаемом устройстве.

Этот тип событий поддерживается в операционных системах Windows и Linux.

Поля события Connection Close

Поле	Тип	Описание
IoAId	string array	Уникальный идентификатор индикатора атаки
IoAName	string array	Название индикатора атаки
IoAVersion	integer array	Версия индикатора атаки
IoAAlert	string array	Возводится ли алерт при срабатывании данного индикатора атаки.
IoAConfidence	string array	Уровень надежности индикатора атаки в зависимости от вероятности ложных срабатываний. High - высокий, Medium - средний, Low - низкий
IoASeverity	string array	Степень важности индикатора атаки с точки зрения возможного влияния события на безопасность компьютеров или локальной сети организации. High - высокий, Medium - средний, Low - низкий
IoATactics	string array	Тактики матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoATechniques	string array	Техники и подтехники матрицы MITRE ATT&CK®, к которым относится срабатывание данного индикатора атаки
IoAEventIds	string array	Перечень идентификаторов событий, связанных с данным индикатором атаки
IoAEventCount	integer array	Количество событий, связанных с данным индикатором атаки
IoASB	string array	Путь к файлу, который отправится на автообработку в песочницу на основании логики индикатора атаки
EventType	string	Тип события
EventId	string	Уникальный идентификатор события
EventTimestamp	int	Дата и время на хосте (клиенте), где произошло событие (дата указана в UTC)
EventReceivedtimestamp	int	Дата и время получения события на сервере

Поле	Тип	Описание
EventSequenceid	int	Номер последовательности отправленного события
HostId	string	Уникальный идентификатор хоста
HostKscId	string	Идентификатор защищаемого хоста для администрирования через KSC
HostMdrId	string	Идентификатор защищаемого хоста в MDR-решении
HostOsmpId	string	Список идентификаторов серверов OSMP Based XDR решений, к которым подключен защищаемый хост
HostOsFamily	string	Тип операционной системы хоста (Windows, Linux)
HostOsName	string	Название операционной системы хоста
HostOsVersion	string	Версия операционной системы хоста
HostName	string	Имя хоста, на котором было обнаружено событие
HostIp	string	IP адрес хоста, на котором было обнаружено событие
AgentVersion	string	Название продукта, установленного на хосте
AgentKdbTimestamp	int	Временная метка обновления компонентов KDB
AgentSw2Timestamp	int	Временная метка обновления баз компонента SW2
AgentIndexTimestamp	int	Временная метка последнего обновления баз всех компонентов
NetSrcIp	string	Адрес источника ipv4/ipv6
NetSrcPort	int	Номер порта источника
NetDstIp	string	Адрес назначения ipv4/ipv6
NetDstPort	int	Номер порта назначения
NetProtocol	string	IP-протокол
NetDirection	string	Направление сетевого соединения (входящее, исходящее)
NetCreationtime	int	Время создания соединения
NetBytessent	int	Количество отправленных байт за время соединения
NetBytesreceived	int	Количество полученных байт за время соединения
NetDuration	int	Длительность соединения в секундах
ProcessUniqueid	int	Уникальный идентификатор процесса
ProcessId	int	Идентификатор процесса
ProcessCmdline	string	Командная строка процесса
ProcessCreationflags	string	Список флагов созданого процесса
ProcessDirectory	string	Директория, из которой был запущен процесс
ProcessEnvironment	string	Переменные окружения
ProcessProperties	string	Свойства аккаунта, из-под которого был запущен процесс
ProcessFileLnkName	string	Имя LNK файла,из которого был запущен файл текущего процесса
ProcessFileLnkPath	string	Путь к LNK-файлу, из которого был запущен процесс (без имени файла)
ProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен файл текущего процесса
ProcessFileLnkCmdline	string	Командная строка LNK-файла
ProcessFileLnkMd5	string	MD5 хэш содержимого LNK файла, из которого был запущен файл текущего процесса
ProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен текущий процесс
ProcessIntegritylevel	int	Уровень целостности процесса
ProcessType	string	Тип процесса

Поле	Тип	Описание
ProcessUserRealid	int	Действующий идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserRealname	string	Действующее имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, который запустил процесс. Указывается для Linux и macOS
ProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший процесс. Указывается для Linux и macOS
ProcessUserEffectivename	string	Эффективное имя пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего процесс. Указывается для Linux и macOS
ProcessFileName	string	Имя файла запущенного процесса (без пути)
ProcessFilePath	string	Путь к файлу запущенного процесса (без имени файла)
ProcessFileFullname	string	Полное имя файла запущенного процесса (включая полный путь к файлу)
ProcessFileSize	int	Размер файла запущенного процесса
ProcessFileCreationtime	int	Дата/время создания файла запущенного процесса
ProcessFileModificationtime	int	Дата/время последней модификации файла запущенного процесса
ProcessFileAttrModificationtime	int	Время последнего изменения атрибутов исполняемого файла процесса
ProcessFileMd5	string	MD5 хэш файла запущенного процесса
ProcessFileSha256	string	SHA256 хэш файла запущенного процесса
ProcessFileAttr	int	Список атрибутов файловой системы исполняемого файла, от которого был запущен процесс
ProcessFileType	string	Тип файла запущенного процесса
ProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса
ProcessFileEmailSrcAddress	string	Email-адрес отправителя письма, во вложении которого был получен файл запущенного процесса
ProcessFileOwnerUserId	int	Идентификатор пользователя владельца файла
ProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец файла
ProcessFileOwnerUserName	string	Имя пользователя владельца файла
ProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец файла
ProcessFileCapPermitted	string	Набор разрешённых возможностей, доступных исполняемому файлу процесса
ProcessFileCapInheritable	string	Разрешения, наследуемые файлом запущенного процесса
ProcessFileCapEffective	string	Набор эффективных возможностей, которые назначены исполняемому файлу, от которого был запущен процесс
ProcessFileZoneidentifier	int	Идентификатор зоны из альтернативного потока (NTFS) Zone.Identifier, который был назначен при загрузке файла
ProcessFileProductname	string	Имя приложения, указанное в ресурсе VERSIONINFO
ProcessFileProductversion	string	Версия приложения, указанная в ресурсе VERSIONINFO
ProcessFileOriginalname	string	Оригинальное имя файла приложения указанное в ресурсе VERSIONINFO
ProcessFileProductvendor	string	Имя компании, указанное в ресурсе VERSIONINFO
ProcessFileDescription	string	Описание, указанное в ресурсе VERSIONINFO
ProcessFileVersion	string	Версия файла, указанная в ресурсе VERSIONINFO

Поле	Тип	Описание
ProcessFileSignResult	string	Результат проверки подписи: пройдена - true, иначе - false
ProcessFileSignTimestamp	int	Дата и время подписания файла
ProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл запущенного процесса
ProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего данный процесс
ProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа процесса
ProcessUserType	int	Тип аккаунта пользователя, запустившего процесс. Возможные значения: Unknown, Admin, NotAdmin
ProcessUserName	string	Имя пользователя (с доменом), запустившего процесс
ProcessLogonUserId	int	Идентификатор пользователя. Указывается для Linux и macOS
ProcessLogonHostName	string	Полное (FQDN) имя удалённого хоста, с которого залогинился пользователь, запустивший процесс
ParentProcessUniqueid	int	Уникальный идентификатор родительского процесса
ParentProcessId	int	Идентификатор родительского процесса
ParentProcessCmdline	string	Командная строка родительского процесса
ParentProcessCreationflags	string	Список флагов родительского процесса
ParentProcessDirectory	string	Текущая рабочая директория родительского процесса. Указывается для Linux и macOS
ParentProcessFileLnkName	string	Имя (без указания пути) LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkPath	string	Путь к LNK файлу (без имени файла), из которого был запущен родительский процесс
ParentProcessFileLnkFullname	string	Полный путь к LNK файлу, из которого был запущен родительский процесс
ParentProcessFileLnkCmdline	string	Командная строка LNK-файла родительского процесса
ParentProcessFileLnkMd5	string	MD5 хеш LNK файла, из которого был запущен родительский процесс
ParentProcessFileLnkSha256	string	SHA256 хэш LNK файла, из которого был запущен родительский процесс
ParentProcessIntegritylevel	int	Уровень целостности родительского процесса
ParentProcessType	string	Тип родительского процесса
ParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего родительский процесс. Указано для Linux и macOS
ParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший родительский процесс. Ссылочное поле Auditd
ParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего родительский процесс. Ссылочное поле Auditd
ParentProcessFileName	string	Имя исполняемого файла родительского процесса (без пути)
ParentProcessFilePath	string	Полный путь к исполняемому файлу родительского процесса (без имени файла)
ParentProcessFileFullname	string	Полный путь к исполняемому файлу родительского процесса

Поле	Тип	Описание
ParentProcessFileCreationtime	int	Время создания исполняемого файла родительского процесса
ParentProcessFileModificationtime	int	Последнее время, когда файл родительского процесса был изменен
ParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла родительского процесса
ParentProcessFileMd5	string	MD5-хэш исполняемого файла родительского процесса
ParentProcessFileSha256	string	SHA256-хэш исполняемого файла родительского процесса
ParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла родительского процесса
ParentProcessFileType	string	Тип исполняемого файла родительского процесса
ParentProcessFileUrl	string	URL, с которого был загружен исполняемый файл родительского процесса
ParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл родительского процесса был получен как вложение
ParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла родительского процесса
ParentProcessFileOwnerGroupName	string	Имя группы, к которой принадлежит владелец исполняемого файла родительского процесса
ParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла родительского процесса
ParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO ресурс исполняемого файла родительского процесса
ParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла родительского процесса
ParentProcessFileSignResult	string	Результат проверки подписи файла родительского процесса: пройдена - true, иначе - false
ParentProcessFileSignTimestamp	int	Дата и время подписания файла родительского процесса
ParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл родительского процесса
ParentProcessLogonType	string	Тип сеанса входа в систему родительского процесса
ParentProcessLogonSessionId	int	Идентификатор сеанса входа из токена доступа родительского процесса
ParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен родительский процесс
ParentProcessUserName	string	Домен и имя пользователя, запустившего родительский процесс
GrandParentProcessUniqueid	int	Уникальный идентификатор прародительского процесса
GrandParentProcessId	int	Идентификатор прародительского процесса
GrandParentProcessCmdline	string	Командная строка прародительского процесса
GrandParentProcessCreationflags	string	Флаги создания прародительского процесса
GrandParentProcessDirectory	string	Директория, из которой был запущен прародительский процесс
GrandParentProcessFileLnkName	string	Имя LNK-файла, из которого был запущен прародительский процесс (без пути)
GrandParentProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс(без имени файла)
GrandParentProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен прародительский процесс
GrandParentProcessFileLnkCmdline	string	Командная строка LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessFileLnkMd5	string	MD5-хэш LNK-файла, из которого был запущен прародительский процесс

Поле	Тип	Описание
GrandParentProcessFileLnkSha256	string	SHA256 хэш LNK-файла, из которого был запущен прародительский процесс
GrandParentProcessIntegritylevel	int	Уровень целостности прародительского процесса
GrandParentProcessType	string	Тип прародительского процесса
GrandParentProcessUserRealid	int	Действующий (реальный) идентификатор пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealid	int	Действующий (реальный) идентификатор группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserRealname	string	Действующее (реальное) имя пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessGroupRealname	string	Действующее (реальное) имя группы пользователя, запустившего прародительский процесс. Указано для Linux и macOS
GrandParentProcessUserEffectiveid	int	Эффективный идентификатор пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectiveid	int	Эффективный идентификатор группы, к которой принадлежит пользователь, запустивший прародительский процесс. Указывается для Linux и macOS
GrandParentProcessUserEffectivename	string	Эффективное имя пользователя, запустившего прародительский процесс. Ссылочное поле Auditd
GrandParentProcessGroupEffectivename	string	Эффективное имя группы пользователя, запустившего прародительский процесс. Указывается для Linux и macOS
GrandParentProcessFileName	string	Имя исполняемого файла прародительского процесса (без пути)
GrandParentProcessFilePath	string	Полный путь к исполняемому файлу прародительского процесса (без имени файла).
GrandParentProcessFileFullname	string	Полный путь к исполняемому файлу прародительского процесса
GrandParentProcessFileCreationtime	int	Дата и время создания исполняемого файла прародительского процесса
GrandParentProcessFileModificationtime	int	Последнее время, когда исполняемый файл прародительского процесса был изменен
GrandParentProcessFileAttrModificationtime	int	Последнее время, когда были изменены атрибуты исполняемого файла прародительского процесса
GrandParentProcessFileMd5	string	MD5-хэш исполняемого файла прародительского процесса
GrandParentProcessFileSha256	string	SHA256-хэш исполняемого файла прародительского процесса
GrandParentProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла прародительского процесса
GrandParentProcessFileType	string	Тип исполняемого файла прародительского процесса
GrandParentProcessFileUrl	string	URL, откуда был загружен исполняемый файл прародительского процесса. Заполняется если файл прародительского процесса был загружен из интернета
GrandParentProcessFileEmailSrcAddress	string	Адрес отправителя, с которого исполняемый файл прародительского процесса был получен как вложение. Заполняется, если файл прародительского процесса был получен в письме как вложение
GrandParentProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupId	int	Идентификатор группы, к которой принадлежит владелец исполняемого файла прародительского процесса
GrandParentProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла прародительского процесса
GrandParentProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла прародительского процесса
GrandParentProcessFileCapEffective	string	Эффективные возможности исполняемого файла прародительского процесса
GrandParentProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла прародительского процесса

Поле	Тип	Описание
GrandParentProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла прародительского процесса
GrandParentProcessFileSignResult	string	Результат проверки подписи файла прародительского процесса: пройдена - true, иначе - false
GrandParentProcessFileSignTimestamp	int	Дата и время подписания файла прародительского процесса
GrandParentProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым был подписан файл прародительского процесса
GrandParentProcessLogonType	string	Идентификатор сеанса входа из токена доступа прародительского процесса
GrandParentProcessLogonSessionId	int	Идентификатор сессии входа в систему из маркера доступа grand-parent процесса
GrandParentProcessProperties	int	Список свойств аккаунта, из-под которого был запущен прародительский процесс
GrandParentProcessUserName	string	Имя пользователя (с доменом), запустившего прародительский процесс
CreatorProcessUniqueid	int	Уникальный идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessId	int	Идентификатор процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCmdline	string	Командная строка процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessCreationflags	string	Флаги создания процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessDirectory	string	Текущая рабочая директория процесса, который является фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkName	string	Имя LNK-файла (без пути), из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkPath	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkFullname	string	Полный путь к LNK-файлу, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileLnkCmdline	string	Параметры командной строки LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.

Поле	Тип	Описание
CreatorProcessFileLnkMd5	string	MD5-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileLnkSha256	string	SHA256-хеш LNK-файла, из которого был запущен процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessIntegritylevel	int	Уровень целостности процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessType	string	Тип процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealid	int	Реальный идентификатор пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealid	int	Реальный идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserRealname	string	Реальное имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupRealname	string	Реальное имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectiveid	int	Действующий идентификатор процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectiveid	int	Действующий идентификатор группы, к которой принадлежит пользователь, запустивший процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserEffectivename	string	Действующее имя пользователя, запустившего процесс, являющийся фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessGroupEffectivename	string	Действующее имя группы пользователя, запустившего процесс, являющегося фактическим создателем текущего. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileName	string	Имя исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFilePath	string	Полный путь (без имени файла) к исполняемому файлу процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileFullname	string	Полный путь к исполняемому файлу процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). В этом случае передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать в пакете телеметрии и следует смотреть на поля ParentProcess*.
CreatorProcessFileCreationtime	int	Время создания исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileModificationtime	int	Время изменения исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttrModificationtime	int	Время изменения атрибутов исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileMd5	string	MD5-хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSha256	string	SHA256 -хеш исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileAttr	int	Список атрибутов файловой системы для исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileType	string	Тип исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileUrl	string	URL-адрес, с которого был загружен исполняемый файл процесса, являющегося фактическим создателем текущего. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileEmailSrcAddress	string	Адрес отправителя, от которого исполняемый файла процесса, являющегося фактическим создателем текущего процесса, был получен в виде вложения. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessFileOwnerUserId	int	Идентификатор пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupId	int	Идентификатор группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerUserName	string	Имя пользователя владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOwnerGroupName	string	Имя группы владельца исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileCapEffective	string	Набор действующих привилегий исполняемого файла процесса, который является фактическим создателем текущего процесса. Указывается для Linux и macOS. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductname	string	Значение имени продукта из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileOriginalname	string	Оригинальное имя файла из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileProductvendor	string	Значение имени компании из ресурса VERSIONINFO исполняемого файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileDescription	string	Описание из ресурса VERSIONINFO исполняемого файла процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignResult	string	Результат проверки подписи исполняемого файла процесса, являющегося фактическим создателем текущего процесса: пройдена - true, иначе - false. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignTimestamp	int	Дата и время подписания файла процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess).Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessFileSignSubjectname	string	Название организации, выпустившей сертификат, которым подписан файл процесса, являющегося фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Поле	Тип	Описание
CreatorProcessLogonType	string	Тип сеанса входа в систему пользователя, запустившего процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessLogonSessionId	int	Идентификатор сеанса входа из маркера доступа процесса, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessProperties	int	Свойства аккаунта, из-под которого был запущен процесс, который является фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*
CreatorProcessUserName	string	Имя пользователя (с доменом), запустившего процесс, являющийся фактическим создателем текущего процесса. Обычно инициатор создания процесса (ParentProcess) совпадает с фактическим создателем (CreatorProcess). Тогда передаваемые в составе телеметрии поля CreatorProcess* будут отсутствовать и следует смотреть на поля ParentProcess*

Работа с событиями

Раздел **Поиск угроз** содержит инструменты, которые помогут вам в поиске угроз и уязвимостей путем анализа событий.

Гранулярный доступ к событиям

В KUMA есть возможность обеспечить гранулярный доступ к событиям для пользователей с разными правами. Доступ к событиям регулируется на уровне пространств хранилища.

Вы можете назначить пользователям пространства в разделе **Доступ к пространствам**. После обновления до последней версии всем существующим пользователям будет назначен набор пространств "All spaces", то есть доступны все пространства без ограничений. Событие содержит идентификатор тенанта и пространства, поэтому пользователь должен обладать правами на соответствующий тенант и пространство, чтобы событие было доступно.

Следует учитывать следующие особенности отображения хранилищ:

- Если хранилища нет в разделе **Активные сервисы**, хранилище и его пространства не отображаются в списке набора пространств.
- Если сервис хранилища был остановлен с помощью команды `systemctl stop kuma-<идентификатор хранилища>`, хранилище и его пространства не отображаются в списке набора пространств.
- Если хранилище было запущено и далее удалено с помощью команды `uninstall`, хранилище и его пространства продолжают отображаться в списке набора пространств.

В списке событий вы можете добавить в таблицу отображение поля **SpaceID**, в нем будет отображаться наименование пространства. Пространство событий аудита отображается как KUMA Audit. KUMA Default – пространство внутри каждого хранилища, куда передаются все события, если в хранилище отсутствуют настроенные пространства или если событие не попадает под условия наполнения существующих пространств.

При экспорте списка событий в файл TSV для пространств отображаются идентификатор и наименование пространства.

Чтобы разграничить доступ:

1. Настройте наборы пространств.

   Вы можете создать, изменить, удалить набор пространств. В результате выполнения этих действий формируются события аудита.

2. Настройте права доступа к набору пространств. Вы можете выдать или отозвать права доступа для выбранных пользователей.

Создание набора пространств

Чтобы создать набор пространств:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Доступ** → **Доступ к пространствам**.

2. В открывшемся окне нажмите на кнопку **Добавить**.

3. В открывшемся окне **Создание набора пространств** укажите значения для следующих параметров:

   a. В поле **Название** укажите название набора пространств. Допустимо использовать до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Пространства** выберите пространства, которые вы хотите включить в набор, установив флажок рядом с названием пространства. Чтобы удалить пространство из набора, снимите флажок.

   c. Если вы хотите, чтобы набор пространств по умолчанию был доступен всем пользователям, которым не назначен ни один из наборов, установите флажок **Установить по умолчанию**.

      После создания набор будет использоваться в качестве набора про умолчанию. В списке наборов пространств он будет отмечен как набор по умолчанию: в столбце **По умолчанию** будет указано значение **Да**.

      Набор по умолчанию может быть только один. Если вы установите флажок **Установить по умолчанию** в параметрах другого набора и сохраните параметры, произойдет переназначение.

4. Нажмите **Создать**.

Набор пространств создан и отображается в списке пространств. После создания набора пространств в KUMA формируется событие аудита.

Теперь необходимо выдать пользователям права доступа к созданному набору пространств.

Редактирование набора пространств

Чтобы изменить набор пространств:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Доступ** → **Доступ к пространствам**.

2. В открывшемся окне нажмите на нужный набор пространств.

3. В открывшемся окне **Редактирование набора пространств** укажите значения для следующих параметров:

   a. В поле **Название** укажите название набора пространств. Допустимо использовать до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Пространства** выберите пространства, которые вы хотите включить в набор, установив флажок рядом с названием пространства. Чтобы убрать пространство из набора, снимите флажок.

   c. Если вы хотите, чтобы набор пространств по умолчанию был доступен всем пользователям, которым не назначен ни один из наборов, установите флажок **Установить по умолчанию**.

      После сохранения параметров набор будет использоваться в качестве набора про умолчанию. В списке наборов пространств он будет отмечен как набор по умолчанию: в столбце **По умолчанию** будет указано значение **Да**.

      Набор по умолчанию может быть только один. Если вы установите флажок **Установить по умолчанию** в параметрах другого набора и сохраните параметры, произойдет переназначение.

4. Нажмите **Сохранить**.

Набор пространств сохранен и отображается в списке пространств.

Измененный набор пространств доступен всем пользователям, которым был выдан доступ к первоначальному набору пространств. Вы можете регулировать доступ к измененному набору пространств и выдать или отозвать права доступа с помощью кнопки **Управление доступом**.

Удаление набора пространств

Чтобы удалить набор пространств:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Доступ** → **Доступ к пространствам**.

2. В открывшемся окне **Доступ к пространствам** установите флажок рядом с нужным набором пространств.

   Если вы хотите удалить все наборы пространств, установите флажок **Выбрать все** в левой верхней части списка и нажмите **Удалить**.

   > Набор пространств по умолчанию и набор All spaces удалить невозможно.

3. Нажмите **Удалить**.

   Набор пространств удален и больше не отображается в списке пространств. После удаления набора пространств в KUMA формируется событие аудита.

Если у пользователей был доступ только к удаленному набору пространств и доступа к другим наборам нет, таким пользователям будут автоматически выданы права доступа к набору пространств по умолчанию.

Выдать права доступа к набору пространств

Чтобы выдать права доступа к набору пространств:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Доступ** → **Доступ к пространствам**.

2. Выберите набор пространств в списке, установив рядом флажок, и нажмите на кнопку **Управление доступом** на панели инструментов.

3. В открывшемся окне **Пользователи** нажмите **Добавить пользователей**.

4. В открывшемся окне **Добавить пользователей** выберите в списке пользователей, которым вы хотите выдать доступ к набору пространств, и нажмите **Добавить**.

   Если вы хотите выдать права доступа к выбранному набору пространств всем пользователям, нажмите на флажок в левом верхнем углу и выберите один из вариантов: **Выбрать все на странице** или **Выбрать все** и нажмите **Добавить**.

   Отобразится окно подтверждения действий.

5. Если вы хотите выдать права указанным пользователям, в окне подтверждения действий нажмите **Выдать**.

Указанным пользователям выданы права доступа к набору пространств.

Отозвать права доступа к набору пространств

Чтобы отозвать права доступа к набору пространств:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Доступ к пространствам**.

2. Выберите набор пространств в списке, установив рядом флажок, и нажмите на кнопку **Управление доступом** на панели инструментов.

3. В открывшемся окне **Пользователи** выберите нужных пользователей, установив рядом флажок и нажмите **Удалить**.

   Если вы хотите отозвать права доступа к выбранному набору пространств у всех пользователей в списке, нажмите на флажок в левом верхнем углу и выберите один из вариантов: **Выбрать все на странице** или **Выбрать все** и нажмите **Удалить**.

   Отобразится окно подтверждения действий.

4. Если вы хотите отозвать права для указанных пользователей, в окне подтверждения действий нажмите **Отозвать**.

Для указанных пользователей отозваны права доступа к набору пространств.

Если у пользователей нет прав доступа к другим наборам пространств, им будут автоматически выданы права доступа к набору по умолчанию.

Сценарии применения

Перенос данных в последнюю версию KUMA с возможностью разграничения доступа к событиям

Цель: Обновить версию продукта.

Действие: Администратор обновляет версию KUMA до версии 4.0.

Результат: Доступность событий для пользователей не меняется, всем пользователям доступны события в тех тенантах, где у пользователей есть разрешение на просмотр списка событий. При добавлении новых пользователей, тенантов или пространств все пользователи видят события тенантов в соответствии с разрешениями на просмотр списка событий без дополнительных ограничений.

Ограничение доступа к пространствам для всех пользователей

Цель: В установке есть пространства, доступ к которым должны иметь не все пользователи. Требуется добиться, чтобы текущие и новые пользователи не имели доступа к таким пространствам.

Действие: Администратор создает новый набор пространств, включающий в себя те пространства, к которым доступ должен быть у всех пользователей. Каждое пространство задается как кортеж: clusterID, tenantID, spaceID. Таким образом можно собрать из конечного числа пространств набор пространств. После создания набора администратор устанавливает этот набор как набор по умолчанию.

Результат: Для всех пользователей, у которых явно не указан набор пространств, в том числе для новых пользователей, доступ к событиям дополнительно ограничивается в соответствии с набором пространств по умолчанию. То есть им доступны события в тенантах, где у пользователей есть право на просмотр списка событий, и находящиеся в пространствах, указанных в наборе по умолчанию.

Разрешение на просмотр всех событий для некоторых пользователей

Цель: В KUMA установлен набор по умолчанию, явно указывающий только конечное число пространств. Также в KUMA есть пользователи, которые должны иметь доступ ко всем событиям без ограничений. Требуется дать возможность этим пользователям просматривать события из пространств, не указанных в наборе по умолчанию.

Действие: Администратор переходит в раздел **Доступ к пространствам** и выбирает набор All spaces, дающий доступ ко всем пространствам без ограничений, и выдает доступ к этому набору выбранным пользователям.

Результат: Пользователи, которым явно был выдан доступ к набору All spaces, теперь не ограничены в доступе к событиям по пространствам. Их доступ к событиям регулируется только правом на просмотр списка событий в соответствии с назначенной ролью. При добавлении новых пространств или тенантов у этих пользователей будет доступ к находящимися в них событиях при условии права на просмотр списка событий в соответствующем тенанте. У пользователей, которым явно не выдан доступ к набору All spaces, доступ к событиям будет ограничиваться в соответствии с набором пространств по умолчанию.

Разрешение на просмотр событий из конечного множества пространств для некоторых пользователей

Цель: В KUMA установлен набор по умолчанию, явно указывающий только конечное число пространств. Некоторым пользователям требуется видеть другой набор пространств, но не все доступные пространства.

Действие: Администратор создает набор пространств, включающий в себя необходимые пространства, и выдает доступ к этому набору выбранным пользователям.

Результат: Доступ пользователей к событиям ограничивается в соответствии с доступным набором пространств. У пользователей, которым явно не выдан доступ к набору, доступ к событиям будет ограничиваться в соответствии с набором пространств по умолчанию.

Дополнение явно указанного набора пространств у пользователя

Цель: Пользователям u1, u2, u3, u4 явно выдан доступ к набору пространств set1, включающий в себя пространства, в которые попадают события Windows и Linux. Пользователям u1 и u2 дополнительно к событиям Windows и Linux требуется просматривать события Cisco и VMware, которые попадают в соответствующие пространства.

Действие: Администратор создает набор пространств set2, включающий в себя пространства, в которые попадают события Cisco и VMware. Администратор назначает пользователям u1 и u2 набор set2 в дополнение к набору set1.

Результат: Пользователям u1 и u2 теперь доступны события из пространств всех доступных им наборов, то есть события из наборов set1 и set2 - Windows, Linux, Cisco, VMware. Доступ пользователей u3 и u4 к событиям не поменялся.

Редактирование набора пространств

Цель: Некоторым пользователям доступен набор пространств (доступ выдан явно или набор является набором по умолчанию). Для всех этих пользователей требуется добавить доступ к определенному пространству, которого нет в наборе, или отозвать доступ к пространству из набора.

Действие: Администратор редактирует существующий набор пространств, добавляя или удаляя из него нужные пространства.

Результат: Все пользователи, которым был выдан доступ к набору, теперь могут просматривать события в соответствии с обновленным набором пространств.

Удаление набора пространств

Цель: Набор пространств перестал быть актуален, его требуется удалить из KUMA.

Действие: Администратор удаляет существующий набор пространств. Набор All spaces не подлежит удалению. Набор пространств, являющийся набором по умолчанию, не подлежит удалению.

Результат: Удаленного набора пространств больше нет в KUMA. Все пользователи, которым явно был выдан доступ к этому набору пространств, теперь имеют доступ к событиям в соответствии с оставшимися доступными наборами пространств. Если у пользователя не осталось наборов пространств, к которым явно был выдан доступ, для такого пользователя доступ к событиям регулируется в соответствии с набором по умолчанию.

Просмотр таблицы событий

В таблице событий представлен обзор всех событий, полученных Ядром KUMA из источников данных. В таблице отображается список событий, отфильтрованных по выполненному SQL-запросу.

Чтобы просмотреть таблицу событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

2. При необходимости отфильтруйте тенанты. По умолчанию фильтр тенантов выключен и в таблице событий отображаются события, относящиеся ко всем тенантам, к которым у вас есть права доступа на **Чтение**. Чтобы применить фильтр для тенантов:

   a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

      Откроется список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

      В таблице событий отображаются только события, относящиеся к выбранным тенантам.

   Отобразится таблица событий. Дополнительные сведения о столбцах таблицы см. в модели данных нормализованного события.

Поиск и фильтрация событий

При поиске событий создается событие аудита для запросов, выполняемых вручную.

События аудита не создаются для запросов, инициированных панелями мониторинга, отчетами или правилами сбора и анализа данных. Запросы REST API на получение событий также не генерируют событий аудита.

При использовании параметра GROUP BY в момент раскрытия группы создается событие аудита, поскольку для этого выполняется дополнительный запрос.

Если выбран вариант **Запуск в фоновом режиме**, создаются два события аудита: Event Read Attempt и Search Query Cancelled.

Для поиска и фильтрации событий измените SQL-запрос в поле поиска и нажмите на кнопку **Выполнить запрос**. Вы можете ввести SQL-запрос вручную или сгенерировать его с помощью конструктора запросов.

В SQL-запросах поддерживается агрегирование и группировка данных.

Вы можете добавить условия фильтрации к уже сформированному SQL-запросу в окне просмотра статистики, в таблице событий и в области сведений о событии.

Чтобы изменить параметры фильтрации из окна Статистика:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Откройте область деталей **Статистика угроз** одним из следующих способов:

   - В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Статистика угроз**.

   - В таблице событий нажмите на любое значение, а затем в открывшемся контекстном меню выберите пункт **Статистика угроз**.

   В правой части окна откроется область деталей **Статистика угроз**.

3. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.

4. Измените параметры фильтрации, выполнив одно из следующих действий:

   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.

   - Чтобы исключить все события с выбранным значением, нажмите на кнопку −.

Чтобы изменить параметры фильтрации в таблице событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значение параметра события в таблице событий.
3. В открывшемся меню выберите следующие параметры:
   - Чтобы оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.
   - Чтобы исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

Чтобы изменить параметры фильтрации в области сведений о событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на соответствующее событие, чтобы открыть панель сведений о событии.
3. Измените параметры фильтрации, выполнив одно из следующих действий:
   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.
   - Чтобы исключить все события с выбранным значением, нажмите на кнопку −.

В результате параметры фильтрации и таблица событий обновятся, а новый поисковый запрос отобразится в верхней части экрана.

> Когда вы переключаетесь на конструктор запросов, параметры запроса, введенного вручную в поле поиска, не передаются в конструктор, поэтому вам нужно будет создать запрос заново. Запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.

Нажмите на кнопку 🖫, чтобы сохранить текущий фильтр.

Создание SQL-запросов вручную

С помощью строки поиска вы можете вручную создавать SQL-запросы любой сложности для фильтрации событий.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос вручную:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Введите SQL-запрос в поле ввода.

   При вводе имени функции в поле SQL-запроса отображается список функций, которые можно использовать. При выборе функции справа отображается пример ее использования. Например, функция `concatWithSeparator` сопровождается следующим примером:

   ```
   concatWithSeparator('a', '1', '2', '3')
   ```

3. Нажмите на кнопку **Выполнить запрос**.

   Выполнение запроса может занять до нескольких минут.

   Вы также можете запустить выполнение запроса в фоном режиме. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **Запустить в фоне**. В этом случае происходит следующее:

   - Запрос будет добавлен в очередь на выполнение в фоновом режиме, и в разделе **Обнаружение и реагирование** будет создана задача на выполнение этого запроса.
   - Фоновые запросы выполняются с низким приоритетом параллельно.
   - Запрос не может быть отправлен на выполнение в фоновом режиме, если он содержит более 10 000 событий.

   В таблице отобразятся результаты поиска по сформированному SQL-запросу. Результат выполнения запроса в фоновом режиме можно просмотреть в разделе **Обнаружение и реагирование**.

   При необходимости вы можете отменить выполнение запроса, нажав на значок стрелки рядом с кнопкой **Выполнить запрос** и выбрав **Отменить запрос**. При отмене запроса автоматически создается событие аудита.

   При необходимости вы можете отфильтровать события в таблице по периоду.

Чтобы отобразить непечатаемые символы в поле запроса SQL, нажмите любую из следующих комбинаций клавиш:

- **`Ctrl+*/Command+*`**
- **`Ctrl+Shift+8/Command+Shift+8`**

Если вы включите отображение непечатаемых символов в компоненте EDR, другие компоненты (такие как KUMA) не будут автоматически отображать непечатаемые символы, пока вы не перезагрузите вкладки браузера компонентов.

Поддерживаемые функции и операторы

SELECT

Поля событий, которые следует возвращать.

Для **SELECT** в приложении поддержаны следующие функции и операторы:

Функции агрегации: **count**, **avg**, **max**, **min**, **sum**.

Арифметические операторы: **+**, **-**, *****, **/**, **<**, **>**, **=**, **!=**, **>=**, **<=**.

Вы можете комбинировать эти функции и операторы.

Если вы используете в запросе функции агрегации, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, а также получение статистики недоступны.

FROM

Источник данных.

WHERE

Условия фильтрации событий.

- **AND**, **OR**, **NOT**, **=**, **!=**, **>**, **>=**, **<**, **<=**
- **IN**
- **BETWEEN**
- **LIKE**
- **ILIKE**
- **inSubnet**
- **match** (в запросах используется синтаксис регулярных выражений re2, специальные символы необходимо дополнительно экранировать с помощью обратной косой черты "\")

GROUP BY

Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

ORDER BY

Столбцы, по которым следует сортировать возвращаемые данные.

Возможные значения:

- **DESC** – по убыванию.
- **ASC** – по возрастанию.

OFFSET

Пропуск указанного количества строк перед выводом результатов запроса.

LIMIT

Количество отображаемых в таблице строк.

По умолчанию указано значение 250.

> При переключении на конструктор параметры запроса, введенного вручную в строке поиска, не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку Применить в окне конструктора.

> Используемые в поисковых запросах псевдонимы не должны содержать пробелов.

Примеры запросов:

- **SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events с типом **Base** и **Audit**, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250**

  Все события таблицы events, для которых в поле **BytesIn** значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу **Timestamp** в порядке возрастания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат данные, соответствующие заданному шаблону %ssh:% в нижнем регистре, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events для устройств, которые входят в подсеть 00.0.0.0/00, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh.*, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT max(BytesOut) / 1024 FROM `events`**

  Максимальный размер исходящего трафика (КБ) за выбранный период времени.

- **SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250**

  Количество событий и номер порта. События сгруппированы по номеру порта и отсортированы по столбцу **Port** в порядке возрастания. Количество отображаемых в таблице строк – 250.

  Столбцу **ID** в таблице событий присвоено имя Count, столбцу **SourcePort** присвоено имя Port.

- **SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250**

  Если вы хотите указать в запросе специальный символ, вам требуется экранировать его, поместив перед ним обратную косую черту (\).

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh: 'connection', и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

Формирование SQL-запроса с помощью конструктора

Вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос с помощью конструктора:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Нажмите на кнопку , чтобы открыть конструктор запросов.

   Сформулируйте поисковый запрос, указав данные в следующих блоках параметров:

   - **SELECT**

     Поля событий, которые следует возвращать. По умолчанию выбрано значение *, означающее, что необходимо возвращать все доступные поля события. Чтобы настроить отображаемые поля, выберите нужные поля в раскрывающемся списке. Стоит учитывать, что Select * в запросе увеличивает длительность выполнения запроса, но избавляет от необходимости указывать поля в запросе.

     Выбрав поле события, вы можете в поле справа от раскрывающегося списка указать псевдоним для столбца выводимых данных, а в крайнем правом раскрывающемся списке можно выбрать операцию, которую следует произвести над данными: **count**, **max**, **min**, **avg**, **sum**.

   - **FROM**

     Источник данных. Выберите значение **events**.

   - **WHERE**

Условия фильтрации событий.

Чтобы добавить условия и группы, нажмите на кнопки **Добавить условие** и **Добавить группу**. Значение оператора **AND** выбирается по умолчанию в группе условий. Нажмите на значение оператора, чтобы изменить его. Доступные значения: **AND**, **OR**, **NOT**.

Чтобы изменить структуру условий и групп условий, используйте значок ⠿ для перетаскивания выражений.

Чтобы добавить условия фильтрации:

a. В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.

b. В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.

c. Введите значение условия. В зависимости от выбранного типа поля может потребоваться ввести значение вручную, выбрав его из раскрывающегося списка или в календаре.

Чтобы удалить условия фильтрации, нажмите на кнопку **X**. Чтобы удалить условия группы, нажмите на кнопку **Удалить группу**.

- **GROUP BY**

  Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

- **ORDER BY**

  Столбцы, по которым следует сортировать возвращаемые данные. В раскрывающемся списке справа можно выбрать порядок: **DESC** – по убыванию, **ASC** – по возрастанию.

- **LIMIT**

  Количество отображаемых в таблице строк.

  По умолчанию указано значение 250.

  Если при фильтрации событий по периоду, указанному пользователем, количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить**.

   Текущий SQL-запрос будет перезаписан. Сгенерированный SQL-запрос отображается в поле поиска.

   Чтобы сбросить параметры конструктора, нажмите на кнопку **Запрос по умолчанию**.

   Чтобы закрыть конструктор, не перезаписывая существующий запрос, нажмите на кнопку .

4. Для отображения данных в таблице нажмите на кнопку **Выполнить запрос**.

   Выполнение запроса может занять до нескольких минут.

Вы также можете запустить выполнение запроса в фоном режиме. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **Запустить в фоне**. В этом случае происходит следующее:

- Запрос будет добавлен в очередь на выполнение в фоновом режиме, и в разделе **Обнаружение и реагирование** будет создана задача на выполнение этого запроса.
- Фоновые запросы выполняются с низким приоритетом параллельно.
- Запрос не может быть отправлен на выполнение в фоновом режиме, если он содержит более 10 000 событий.

В таблице отображаются результаты поиска по сформированному SQL-запросу. Результат выполнения запроса в фоновом режиме можно просмотреть в разделе **Обнаружение и реагирование**.

При необходимости вы можете отменить выполнение запроса, нажав на значок стрелки рядом с кнопкой **Выполнить запрос** и выбрав **Отменить запрос**. При отмене запроса автоматически создается событие аудита.

При переходе в другой раздел веб-интерфейса сформированный в конструкторе запрос не сохраняется. Если вы повторно вернетесь в раздел События, в конструкторе будет отображаться запрос по умолчанию.

Формирование SQL-запроса с помощью SQL-функций KUMA

SQL-функции KUMA позволяют использовать атрибуты активов и учетных записей в поисковых запросах для фильтрации событий, формирования отчетов и виджетов (тип графика **Таблица**). Вы можете обогащать события, используя данные словарей, таблиц, активов и учетных записей с помощью следующих наборов функций:

- Набор функций enrich. Позволяет обогатить результаты запроса полями актива, учетной записи, значениями из словаря с типом **Словарь** и словаря с типом **Таблица**. Набор функций `enrich` включает в себя следующие функции:
  - `enrich_assets`;
  - `enrich_accounts`;
  - `enrich_table`;
  - `enrich_dictionary`.

- Набор функций lookup. Позволяет добавить в поисковый запрос условия по активам и учетным записям. Набор функций `lookup` включает в себя следующие функции:
  - `lookup_assets`;
  - `lookup_accounts`;
  - `lookup_assets_category`.

Максимальное количество событий в одном запросе – 10 000.

Использование набора функций enrich в SQL-запросах

Набор функций `enrich` (см. таблицу ниже) применяется в блоке `SELECT` SQL-запроса для обогащения результатов.

При использовании этого набора функций вы не можете группировать события по обогащенным полям.

Обогащаемые функциями виджеты и отчеты должны принадлежать не более чем одному тенанту.

Значения полей актива, которые указываются в SQL-запросах, являются регистрозависимыми.

Описание набора функций enrich

Функция	Поле события	Поле актива	Описание

`enrich_assets`	`DeviceAssetID`
	`DestinationAssetID`
	`SourceAssetID`
		`name`
		`os`
		`osBuild`
		`ipAddress`
		`macAddress`
		`fqdn`
		`source`
		`software`
		`cii`
		`ramSize`
		`kscLastAvBasesUpdate`
		`kscLastInfoUpdate`
		`kscLastUpdate`
		`kscLastSystemStart`
		`kscStatusMask`
		`kscRtProtectionState`
		`kscEncryptionState`
		`kscAntiSpamStatus`
		`kscEmailAvStatus`
		`kscDlpStatus`
		`kscStatusID`
		`kscEdrStatus`
		`lastVisible`
		`aistatus`
		`aiscore`
			Позволяет обогатить результат запроса полями актива на основании указанного в функции идентификатора.
			Пример
			`enrich_assets(DeviceAssetID, name)`

Функция	Поле события	Поле актива	Описание
enrich_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name uac	Позволяет обогатить результат запроса полями учетной записи на основании указанного в функции идентификатора. Пример enrich_account(SourceAccountID, name) Функция доступна только для тенантов, у которых включено обогащение с помощью LDAP.
enrich_table	Любое	–	Позволяет обогатить результат запроса значениями из словаря с типом **Таблица** на основании полей событий в ответе от кластера ClickHouse. Пример enrich_table('Main/some-table', [DeviceProduct], 'value') Ключевой может быть только один столбец таблицы, но ключ записи может быть составным. Пример enrich_table('Main/Dictionary', [BytesOut|BytesIn], 'value2') Функция enrich_table возвращает только один столбец таблицы. Если надо вызвать больше столбцов, вызовите функцию повторно с указанием нужных полей.
enrich_dictionary	Любое	—	Позволяет обогатить результат запроса значениями из словаря с типом **Словарь** на основании полей событий в ответе от кластера ClickHouse. Пример 1 enrich_dictionary('Main/some-dict', [SourceAddress] Пример 2 enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress]) Вы можете посмотреть путь до словаря в разделе **Ресурсы** → **Словари**.

Вы можете задавать функцию enrich при ручном создании SQL-запросов.

Примеры запросов с функцией enrich:

Все события таблицы `events` с полями событий `Name` и `Message`, а также с полями актива `macAddress` и `osBuild` для обогащения результата данными актива. Количество отображаемых в таблице строк – 250.

```
SELECT Name,
Message,
   enrich_assets(DeviceAssetID, macAddress),
   enrich_assets(DeviceAssetID, osBuild)
FROM `events`
WHERE DeviceAssetID != ''
LIMIT 250
```

Все события таблицы `events` с полями событий `SourceUserName` и `SourceAddress`, а также со значениями поля `mobile` для обогащения результата данными учетной записи. Количество отображаемых в таблице строк – 10.

```
SELECT SourceUserName,
SourceAddress,
   enrich_accounts(SourceAccountID, mobile) as mobile
FROM `events`
WHERE SourceAccountID != ''
LIMIT 10
```

Все события таблицы `events` с полями событий `DeviceProduct` со значениями из таблицы **Main/[OOTB] Linux. Auditd record types**. Отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 1000.

```
SELECT DeviceProduct,
   enrich_table('Main/[OOTB] Linux. Auditd record types', [DeviceProduct], 'Description') as HTTP
FROM `events` WHERE Type!=4
LIMIT 1000
```

Все события таблицы `events` с полями событий `DeviceAction` со значениями из словаря **Main/[OOTB] KEDR**. Количество отображаемых в таблице строк – 255.

```
SELECT DeviceAction,
   enrich_dictionary('Main/[OOTB] KEDR. AccountType', [BytesOut]) as accountType
FROM `events` WHERE Type!=4
LIMIT 255
```

Использование набора функций lookup в SQL-запросах

Набор функций `lookup` (см. таблицу ниже) применяется в блоке `WHERE` SQL-запроса для добавления в поисковый запрос условий по активам и учетным записям.

В запросы, содержащие функцию `lookup`, KUMA автоматически добавляет в выражение `SELECT` поле `*ID`, которое используется в функции `lookup` в запросе. Например, в запрос, содержащий функцию `lookup_assets(DeviceAssetID, osBuild, '=', '19045.000000')`, в выражение `SELECT` будет добавлено поле `DeviceAssetID`.

> В запросах, содержащих функцию `lookup`, рекомендуется прописывать в функции `SELECT` список полей, которые необходимо возвращать. Не рекомендуется использовать в функции `SELECT` значение *. В этом случае будут возвращаться все доступные поля, что может значительно увеличить длительность выполнения запроса.

Тип функции	Поле события	Поле актива	Оператор	Описание
lookup_assets	DeviceAssetID SourceAssetID DestinationAssetID	name os osBuild source cii ramSize kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus aistatus aiscore	=	Позволяет добавить в резул условия по активам, значени совпадают со значением, ука запросе. Для значений, которые являк надо указывать строку с нео числом. Например: lookup_assets(DeviceAss '=', '19045.000000') lookup_assets(DeviceAss '=', '3241234234')
		kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart lastVisible ramSize aiscore	< > <= >=	Позволяет добавить в резул условия по активам, значени • меньше значения, указан • больше значения, указан • меньше или равно значе в запросе; • больше или равно значе в запросе. Для значений, которые являк надо указывать строку с нео числом. Например: lookup_assets(DeviceAss '>', '50') Значения, которые являются указывать в следующих форм • Количество секунд: lookup_assets(Device lastVisible, '>', '1 • Количество миллисекунд lookup_assets(Device lastVisible, '<', '1725971837834') • Количество дней: lookup_assets(Device lastVisible, '<', 'n
		name os osBuild fqdn software	like	Позволяет добавить в резул условия по активам, значени соответствуют like-выражен запросе. Подробнее об операторе like Language Expressions. lookup_assets(Destinati name, 'like','test.compa
		ipAddress macAddress fqdn software kscStatusMask	in	Позволяет добавить в резул условия по активам, значени соответствует значению, ука запросе. Например: lookup_assets(DeviceAss 'in', ['test_fqdn1.compa 'test_fqdn2.company.ru']

Тип функции	Поле события	Поле актива	Оператор	Описание
		`ipAddress`	`insubnet`	Позволяет добавить в резул условия по активам с IP-адре входят в указанную подсеть. указывается в формате CIDR Например: `lookup_assets(DeviceAss ipAddress, 'insubnet',`
		`ipAddress`	`inrange`	Позволяет добавить в резул условия по активам, IP-адрес попадает в указанный диапаз Первый указанный в запросе является начальным, второй Например: `lookup_assets(DeviceAss ipAddress, 'inrange', [ '192.168.1.184'])` По результатам выполнения отфильтрованы активы с IP-а находящимися в диапазоне с 192.168.1.184.

Тип функции	Поле события	Поле актива	Оператор	Описание
lookup_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn title division department manager location company street_address physical_delivery_office_name uac	=	Позволяет добавить в резул условия по учетным записям которых совпадают со значе в запросе. Для значений, которые являк надо указывать строку с нео числом. Например: lookup_accounts(SourceA employee_id, '=', '1545
		name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name	like	Позволяет добавить в резул условия по учетным записям которых соответствуют like- указанному в запросе. Подробнее об операторе like Language Expressions. lookup_accounts(Destina name, 'like', '_ccount1

Тип функции	Поле события	Поле актива	Оператор	Описание

`lookup_assets_category`	`DeviceAssetID`
	`SourceAssetID`
	`DestinationAssetID`
		–	–	Позволяет найти все событи связанные активы находятся папке.
				Например:
				`lookup_assets_category( ['Main/Business Impact']`
				где `Main` – это название тен `Impact` – название папки.

Примеры SQL-запросов с функцией lookup

Вы можете задавать функцию `lookup` при ручном создании SQL-запросов. Примеры запросов с функцией `lookup`:

- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также с полем актива `fqdn`, значение которого содержит подстроку `win10`. Количество отображаемых в таблице строк – 250.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets(DeviceAssetID, fqdn, 'match', 'win10')
LIMIT 250
```
- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также со значениями поля `EmployeeID`, значение которого равно `15452`. Количество отображаемых в таблице строк – 10.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE SourceAccountID != ''
AND lookup_accounts(SourceAccountID, employee_id, '=', '15452')
LIMIT 10
```
- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также с указанием папки, в которой находится актив. Количество отображаемых в таблице строк – 100.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets_category(DeviceAssetID, ['Main/Business Impact'])
LIMIT 100
```

Просмотр сведений о событии

Чтобы открыть сведения о событии, выберите событие в таблице событий в разделе **Поиск угроз** или на странице деталей алерта.

Панель **Информация о событии** отображается в правой части окна веб-интерфейса и содержит список параметров события со значениями. В этой области вы можете:

- Включить выбранное поле в поиск или исключить его из поиска, нажав на + или на – рядом со значением параметра.
- Найти похожие события и добавить или удалить правило запрета, нажав на значения **FileHash** и **DeviceCustomString**.
- При интеграции с Kaspersky CyberTrace и Kaspersky Threat Intelligence Portal вы можете добавить в пользовательские сведения о киберугрозах CyberTrace и отобразить информацию из Поиска угроз (Threat Lookup), нажав на значения **FileHash** и **DeviceCustomString**.
- Просмотрите параметры службы, зарегистрировавшей событие, нажав на значение **Служба**.
- Просмотреть список алертов или инцидентов, связанных с устройством, нажав на значение **DeviceAssetID** и выбрав **Сведения об активе**. В открывшемся окне **Информация об устройстве** нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты** в зависимости от того, что вы хотите просмотреть.

- Просмотр списка IOA-правил, сработавших при создании события; просмотр сведений об этих IOA-правилах, нажав на их названия.

  На открывшейся панели IOA-правило отображаются подробные сведения

  В открывшихся сведениях о правиле IOA доступны следующие действия:

  - Просмотр имени IOA-правила, идентификатора, уровня важности и уровня надежности.
  - Добавление IOA-правила в исключения.
  - Просмотреть информацию о поиске угроз, нажав на кнопку **Найти в Kaspersky TIP**.
  - По нажатию на кнопку **Открыть в** можно просмотреть алерты и инциденты, созданные при срабатывании правила IOA.
  - Просмотреть связанные события, нажав на кнопку **Найти в разделе "Поиск угроз"**.

    По умолчанию события отображаются за 24 часа.

  Вы также можете просмотреть подробную информацию о IOA-правиле в Kaspersky TIP. Для этого в окне сведений о IOA-правиле нажмите на кнопку **Найти в Kaspersky TIP**.

- Включите или выключите компактный режим отображения для `*Label`, нажмите на значок ⚙ и переведите переключатель в нужное положение. По умолчанию переключатель установлен в положение **Развернутый вид**. Если для полей `DeviceCustom*` и `Flex*` выбран режим **Компактный вид**, значение соответствующего поля `*Label` отображается как имя поля, а само поле `*Label` скрывается из списка полей событий. Если значение поля `*Label` отсутствует, отображается исходное название поля. Выбранный режим отображения сохраняется после обновления страницы и выхода из раздела **Поиск угроз**.

В панели **Информация о событии** вместо идентификатора отображается имя описываемого объекта в значениях следующих параметров. Если вы измените параметры фильтра в панели **Информация о событии**, в SQL-запрос будет добавлен идентификатор объекта, а не его имя:

- TenantID
- SeriviceID
- DeviceAssetID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

Сохранение и выбор конфигурации фильтра событий

Вы можете сохранить текущую конфигурацию фильтра, включая временной фильтр, конструктор запросов и параметры таблицы событий, для использования в будущем. Сохраненные конфигурации фильтров доступны вам и другим пользователям, имеющим соответствующие права доступа.

Чтобы сохранить текущие параметры фильтра, запроса и периода

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите пункт **Сохранить текущий фильтр**.
3. В открывшемся окне **Новый фильтр** введите название конфигурации фильтра в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
4. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный фильтр.
5. Нажмите на кнопку **Сохранить**.

   Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите нужный фильтр.

Чтобы сохранить текущие параметры фильтра, запроса и параметры таблицы событий

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий.
3. Нажмите на пункт **Сохранить текущий пресет**.
4. В открывшемся окне **Новый пресет** введите название пресета в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
5. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный пресет.
6. Нажмите на кнопку **Сохранить**.

   Конфигурация пресета сохранена.

Чтобы выбрать ранее сохраненную конфигурацию пресета

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий. Выберите вкладку **Пресеты**.
3. Выберите необходимый пресет.

Чтобы удалить ранее сохраненную конфигурацию фильтра для всех пользователей

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок рядом с поисковым запросом.
3. Нажмите на значок рядом с конфигурацией, которую нужно удалить.
4. Нажмите на кнопку **OK**.

Фильтрация событий по периоду

Вы можете указать период для отображения событий.

Чтобы отфильтровать события по периоду:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Откройте второй раскрывающийся список в верхней части окна.
3. Укажите период. Вы можете выбрать предопределенные периоды относительно текущей даты и времени или указать необходимый период, используя поля **Начало периода** и **Конец периода** или выбрав даты в календаре.
4. Нажмите на кнопку **Применить**.

Экспорт событий

Вы можете экспортировать информацию о событиях в файл TSV. Выборка событий, которые будут экспортированы в файл TSV, зависит от параметров фильтра. Информация экспортируется из столбцов, которые отображаются в таблице событий. Столбцы в экспортируемом файле заполняются доступными данными, даже если они не отображались в таблице событий в разделе **Поиск угроз** из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в раскрывающемся списке выберите **Экспортировать в CSV**.

   Новая задача экспорта файла TSV создана в разделе KUMA **Диспетчер задач**.
3. В разделе KUMA, в подразделе **Диспетчер задач** найдите созданную вами задачу.
4. Нажмите на название типа задачи и выберите в раскрывающемся списке пункт **Загрузить**.

   Файл TSV будет загружен с использованием параметров вашего браузера. По умолчанию имя файла event-export-<date>_<time>.tsv.

Файл сохранен в соответствии с параметрами вашего браузера.

Просмотр событий аудита и настройка уведомлений

Аудит – это процесс мониторинга, регистрации и анализа действий пользователей и системных операций, направленных на обеспечение безопасности и контроль изменений.

Kaspersky EDR Expert получает события аудита от компонентов решения автоматически, дополнительная настройка не требуется. Во время развертывания решения Kaspersky EDR Expert создает предустановленный коллектор **[OOTB] Kaspersky OSMP** в корневом тенанте. У этого коллектора есть предустановленный коннектор **[OOTB] Kaspersky OSMP** и предустановленный нормализатор **[OOTB] Kaspersky OSMP audit**. Коллектор отправляет события аудита в пространство хранилища **KUMA Audit**. Это пространство хранилище создается автоматически.

> Kaspersky EDR Expert получает события аудита только в том случае, если вы указали действительный лицензионный ключ для SIEM-компонента в параметре `license` во время развертывания на одном узле, развертывания на нескольких узлах или в интерфейсе решения.

При необходимости вы можете настроить параметры хранилища для событий аудита, если создаете набор ресурсов для хранилища.

Подробная информация о параметрах и типах действий аудита приведена в статье События аудита.

Как просмотреть и экспортировать события аудита в файл

События аудита доступны в разделе **Мониторинг** → **Поиск угроз**.

Если вы хотите, чтобы в таблице событий отображались только события аудита, выполните одно из следующих действий:

- В таблице событий в поле **EventType** установите значение `Audit`.
- Разграничьте доступ к пространству с помощью событий аудита.

  Для этого перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Доступ к пространствам** и настройте права доступа к пространству KUMA Audit. Только пользователи, которым предоставлены права доступа к пространству, смогут просматривать события аудита в разделе **Поиск угроз**.

После фильтрации событий аудита в таблице вы можете экспортировать события в файл.

Как настроить уведомление по электронной почте о событиях аудита

Как только происходит событие, например, пользователь выполняет более пяти неудачных попыток входа в Консоль OSMP, срабатывает предопределенное правило корреляции и создается алерт.

Если вы хотите получать уведомления об алертах по электронной почте, вам нужно создать шаблон уведомления. В панели **Создать шаблон электронной почты** укажите следующие параметры:

- В раскрывающемся списке **Тип события** выберите тип шаблона уведомления **Создание алерта**.
- В раскрывающемся списке **Правила корреляции** выберите предустановленное правило корреляции.

События аудита

События аудита отображаются в разделе **Поиск угроз** и могут включать типы действий, перечисленные в таблице ниже.

Тип действия	Название действия	Параметры и описание
Работа компонента	`Service start`	
	`Service stop`	`reason` Причина прерывания службы, если доступно.
Операции с алертами	`Alert assigning`	• `alert_id` Идентификатор алерта, с которым выполняется действие. • `group_name` Имя группы, которой назначен алерт. • `group_id` Идентификатор группы, которой назначен алерт.
	`Changing alert status`	• `alert_id` Идентификатор алерта, с которым выполняется действие. • `alert_status` Предыдущий статус алерта. • `new_alert_status` Новый статус алерта.
	`Alert auto assigning`	• `alert_id` Идентификатор алерта, с которым выполняется действие. • `account_name` Имя пользователя, которому назначен алерт. • `account_id` Идентификатор пользователя, которому назначен алерт.

Операции с инцидентами	`Creating incident`	`incident_id` Идентификатор инцидента, с которым выполняется действие.
	`Incident assigning`	• `incident_id` Идентификатор инцидента, с которым выполняется действие. • `group_name` Имя группы, которой назначен инцидент. • `group_id` Идентификатор группы, которой назначен инцидент.
	`Changing incident status`	• `incident_id` Идентификатор инцидента, с которым выполняется действие. • `incident_status` Предыдущий статус инцидента. • `new_incident_status` Новый статус инцидента.
	`Merge incidents`	`incident_id` Идентификатор целевого инцидента после слияния.
	`Incident auto assigning`	• `incident_id` Идентификатор инцидента, с которым выполняется действие. • `account_name` Имя пользователя, которому назначен инцидент. • `account_id` Идентификатор пользователя, которому назначен инцидент.
Операции с правилами сегментации	`Creating segmentation rule`	`rule_name` Имя правила сегментации.
	`Changing segmentation rule`	
	`Enabling segmentation rule`	
	`Disabling segmentation rule`	
	`Deleting segmentation rule`	
Операции с правилами сегментации	`Creating aggregation rule`	`rule_name` Идентификатор правила агрегации.
	`Changing aggregation rule`	
	`Enabling aggregation rule`	
	`Disabling aggregation rule`	
	`Deleting aggregation rule`	
Уведомления по электронной почте	`Creating e-mail templates`	`subject` Тема шаблона электронного письма, с которым выполняется действие.
	`Enabling e-mail templates`	
	`Disabling e-mail template`	
	`Changing e-mail templates`	
	`Deleting e-mail templates`	

Settings	Enabling auto send to SB by IOA trigger	tenant_name Имя тенанта, с которым выполняется действие.
	Disabling auto send to SB by IOA trigger	
	Turning on the Assign "Untrusted" status to alerts toggle switch	
	Turning off the Assign "Untrusted" status to alerts toggle switch	
	Enabling the use of KSN	
	Disabling the use of KSN	
	Enabling the use of KPSN	
	Disabling the use of KPSN	
	Enabling the use of MDR	
	Disabling the use of MDR	
	Configuring the connection of OSMP to a local reputation database of KPSN	
	Enabling auto send to SB	
	Disabling auto send to SB	
	Enabling manual send to SB	
	Disabling manual send to SB	
	Selecting a database update source	
	Updating database manually	version_of_updated_databases Версия антивирусных баз.
	Auto updating database	
	Changing passwords for archives	
	Enabling the required password change	
	Disabling the required password change	
	Enabling user password change	period Количество дней, по истечении которых пароль должен быть изменен.
Управление тенантами	Creating tenant	tenant_name Имя тенанта.
	Changing tenant	
	Bind Administration Server	
	Changing integration KATA/KEDR	integration_parameters Параметры интеграции.
	Changing integration TIP	
	Changing custom integration	

	Changing integration	
Хранилище	Uploading file to storage	• file_name Имя файла. • alert_id Идентификатор инцидента, с которым выполняется действие. • incident_id Идентификатор инцидента, с которым выполняется действие.
	Downloading file from storage	
	Deleting file from storage	
	Auto deleting file from storage	
Параметр	Configuring an IOC scan schedule	
Правила запрета	Uploading prevention rules from file	• file_name Имя файла. • count Количество правил запрета, созданных после импорта файла.
	Creating a prevention rule	file_name Имя файла.
	Modifying a prevention rule	
	Enabling the use of a prevention rule	
	Disabling the use of a prevention rule	
	Removing a prevention rule	
Плейбуки	Creating a playbook	playbook_name Название плейбука.
	Removing a playbook	
	Changing the operation mode	
YARA	Uploading a YARA file	file_name Имя файла.
	Downloading a YARA rule	rule_name Имя YARA-правила.
	Changing YARA rule	
	Enabling the automatic use of YARA rules	
	Disabling the automatic use of YARA rules	
	Deleting a YARA rule	
IOC	Uploading an IOC file	file_name Имя файла.
	Downloading an IOC rule	rule_name Имя IOC-правила.
	Changing IOC rule	
	Enabling the automatic use of IOC rules	
	Disabling the automatic use of IOC rules	
	Deleting an IOC rule	

Работа с TLS-сертификатами	`Generating a TLS certificate for the Endpoint Agent component`	
	`Uploading a TLS certificate for the Endpoint Agent component`	
	`Deleting a TLS certificate for the Endpoint Agent component`	
	`Downloading the TLS certificate of the server`	
Параметры Sandbox	`OS set of virtual machines changed`	`sb_name` Название Sandbox.
	`Creating a request for connection to the server with the Sandbox component`	
	`Enabling a connection with the Sandbox component`	
	`Disabling a connection with the Sandbox component`	
	`Deleting a connection with the Sandbox component`	
	`Renaming the Sandbox server`	• `new_sb_name` Новое имя Sandbox. • `sb_ip` IP-адрес Sandbox.
Правила Sandbox	`Creating a file scanning rule in custom images`	`virtual_machine_name` Имя виртуальной машины.
	`Enabling a file scanning rule in custom images`	
	`Disabling a file scanning rule in custom images`	
	`Deleting a file scanning rule in custom images`	
	`Editing a file scanning rule in custom images`	• `virtual_machine_name` Имя виртуальной машины. • `new_virtual_machine_name` Новое имя виртуальной машины, если оно было изменено.
	`Export a file scanning rule in custom images`	`file_name` Имя файла.
	`Import a file scanning rule in custom images`	`file_name` Имя файла.
Распределенное решение	`Assigning the PCN OSMP role`	`tenant_name` Имя тенанта.
	`Assigning the SCN OSMP role`	
	`Creating a request for connection of the SCN OSMP to the PCN OSMP`	
	`Accepting a request for connection of the SCN OSMP to the PCN OSMP`	
	`Rejecting a request for connection of the SCN OSMP to the PCN OSMP`	
	`Confirming the assign PCN role to CN`	

	`Disconnecting an SCN from PCN`	
Операции с учетными записями	`Creating a user account`	• `account_name` Имя пользователя. • `account_id` Идентификатор пользователя. • `account_authorization` Дата и время последнего входа учетной записи, с которой было выполнено действие. • `password_verification` Статус проверки пароля учетной записи, с которой выполняется действие. • `account_expiration_date` Срок действия учетной записи, с которой выполняется действие. Значение всегда равно `01.01.2222`. • `account_status` Статус учетной записи, с которой выполняется действие. • `account_type` Тип учетной записи, с которой выполняется действие.
	`Changing access rights of user account`	
	`Change the password`	
	`Enabling account`	
	`Disabling account`	
	`Deleting an account`	
Аутентификация и авторизация пользователей	Successful login	`administrator_rights` Указывает, есть ли у пользователя права администратора.
	Login denied because the user is not registered	
	Login denied because the user is blocked	
	Login denied because the password is incorrect	
	Login denied because the password attempt limit was exceeded	
	Login denied because the password has expired	
	Log off	

Ретроспективное сканирование

Вы можете использовать ретроспективное сканирование (retroscan), чтобы уточнить ресурсы правил корреляции или проанализировать данные истории.

Вы также можете создавать алерты на основе функции ретроспективного сканирования (retroscan).

Чтобы использовать ретроспективное сканирование:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Ретроспективное сканирование**.

   Откроется панель **Ретроспективное сканирование**.

3. В раскрывающемся списке **Коррелятор** выберите пункт Коррелятор, в который будут передаваться выбранные события.

4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, которые необходимо использовать при обработке событий.

5. Чтобы выполнить действия по реагированию во время обработки событий, включите переключатель **Выполнить действия по реагированию**.

6. Чтобы генерировать алерты во время обработки событий, включите переключатель **Создать алерты**.

7. Нажмите на кнопку **Создать задачу**.

   Задача ретроспективного сканирования создана в разделе KUMA **Диспетчер задач**.

Получение статистики таблицы событий

Вы можете получить статистику по выбранным событиям, отображаемым в таблице событий. Выбранные события зависят от параметров фильтра.

Чтобы получить статистику:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Выполните одно из следующих действий:

   - В верхнем правом углу таблицы событий выберите **Статистика** из раскрывающегося списка ••• .

   - В таблице событий нажмите на любое значение и в контекстном меню выберите пункт **Статистика**.

Отобразится область сведений раздела **Статистика** со списком параметров из текущей выборки событий. Цифры возле каждого параметра означают количество событий с этим параметром в выборке. Если параметр развернут, отображаются пять наиболее часто встречающихся значений. Введите название параметра в **Поля поиска** для фильтрации отображаемых данных.

Окно **Статистика** позволяет изменять фильтр событий.

> При использовании SQL-запросов с группировкой и агрегированием данных для фильтрации событий статистика недоступна.

Реагирование на угрозы

Чтобы выполнить действия по реагированию, просмотреть результат обогащения, которое вы выполнили из плейбука, и запустить плейбуки вручную, вам нужно перейти в раздел **Алерты** или **Инциденты**.

Разделы **Алерты** и **Инциденты** отображаются в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky EDR Expert.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

После выполнения действия по реагированию, вы можете просмотреть историю действий по реагированию.

Действия по реагированию

Действия по реагированию можно запустить одним из следующих способов:

- вручную, как описано в этом разделе;

  Для устройств, на которых не установлено приложение Kaspersky Endpoint Security со встроенным агентом, вы не можете выполнять следующие действия по реагированию: Управление службами, Удаление файла, Сканирование YARA, IOC-проверка, Получение файла из карантина, а также действия по реагированию, описанные в разделе Получение файлов для дальнейшего анализа.

  При реагировании из деталей алерта или инцидента или из таблицы активов вы не можете выбрать архивированные устройства.

- в рамках плейбука.

  В этом случае при создании или изменении плейбука вы можете настроить автоматический запуск действия по реагированию или запросить подтверждение пользователя перед запуском в плейбуке. По умолчанию ручное подтверждение действий по реагированию выключено.

  Если устройство архивируется во время выполнения действия по реагированию, в результате выполнения плейбука отображается сообщение об **ошибке**. Если плейбук запускается для алерта, который включает в себя архивированные устройства, в результате выполнения плейбука отображается предупреждающее сообщение о том, что устройство архивировано.

Прерывание процессов

Действие по реагированию *Прервать процесс* позволяет удаленно завершать процессы на устройствах. Вы можете выполнить действие по реагированию Прервать процесс для наблюдаемых объектов или активов.

Вы можете запустить действие по реагированию Прервать процесс одним из следующих способов:

- Из деталей алерта или инцидента.
- Из сведений об устройстве.

- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.

- Из графа расследования.

  Параметр доступен, если граф расследования построен.

- Из таблицы активов.

- В разделе **История реагирований**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действие по реагированию Прервать процесс, вам должна быть присвоена одна из следующих EDR-ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Реагирование из деталей алерта или инцидента

Чтобы завершить процесс из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.

2. В открывшемся окне выберите вкладку **Активы**.

   Вы также можете перейти на вкладку **Наблюдаемые объекты** и выбрать один или несколько наблюдаемых объектов, для которых вы хотите прервать процесс. Наблюдаемые объекты могут включать хеши MD5 или SHA256.

3. В списке активов выберите одно или несколько устройств.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Прервать процесс**.

5. В открывшейся правой панели выполните следующее:

   a. В поле **Полный путь** укажите полный путь к файлу процесса.

   b. В раскрывающемся списке **Активы** выберите устройства, для которых вы хотите завершить процесс.

      Если на шаге 2 была выбрана вкладка **Активы**, имена устройств, для которых вы установили флажки, по умолчанию указываются в поле **Активы**. Вы можете изменить их или выбрать вариант **Все активы** в раскрывающемся списке **Область действия** для завершения процесса на всех устройствах, принадлежащих тенанту алерта или инцидента (и его дочерним тенантам).

      > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   c. При необходимости настройте следующие параметры в соответствующих полях:

      - Укажите SHA256 или хеш MD5 файла процесса.

        Если на шаге 2 вы выбрали вкладку **Наблюдаемые объекты**, выбранные вами хеши будут указаны по умолчанию. Вы можете их изменить.

      - Напишите описание или комментарий к действию по реагированию.

6. Нажмите на кнопку **Прервать**.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из сведений об устройстве

Чтобы завершить процесс с помощью сведений устройства:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство с файлом, который нужно переместить на карантин.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство с файлом, который нужно переместить на карантин.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из телеметрии события

Чтобы завершить процесс из телеметрии события при его открытии из деталей алерта или инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство с файлом, который нужно переместить на карантин.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку **Найти в разделе "Поиск угроз"**, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.

   > Вы также можете перейти на вкладку **Наблюдаемые объекты** и выбрать один или несколько наблюдаемых объектов, для которых вы хотите прервать процесс. Наблюдаемые объекты могут включать хеши MD5 или SHA256.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Прервать процесс**.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Прервать процесс**.

4. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из графа расследования

Параметр доступен, если граф расследования построен.

Чтобы завершить процесс из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.

2. В открывшемся окне **Детали инцидента** нажмите на кнопку **Посмотреть на графе**.

   Откроется окно **графа расследования**.

3. Нажмите на имя нужного устройства и в раскрывающемся списке выберите **Просмотреть информацию**.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Прервать процесс**.

4. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите **Прервать процесс**.

3. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Процесс прерван. Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение – **Успешно**. Иначе отобразится сообщение об ошибке с информацией о причине.

Если вы хотите просмотреть идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Перемещение файлов на карантин

Для того чтобы предотвратить распространение угрозы, вы можете переместить зараженный файл на карантин одним из следующих способов:

- Из деталей алерта или инцидента.
- Из сведений об устройстве.
- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.

- Из графа расследования.
- Из таблицы активов.
- В разделе **История реагирований**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы переместить файл на карантин, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Реагирование из деталей алерта или инцидента

Чтобы переместить файл на карантин из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство с файлом, который нужно переместить на карантин.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство с файлом, который нужно переместить на карантин.
2. В открывшемся окне выберите вкладку **Активы**.

   Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с файлом, который вы хотите переместить на карантин, и нажать на кнопку **Переместить на карантин**.
3. Установите флажок рядом с устройством с файлом, который нужно переместить на карантин.

   При необходимости вы можете выбрать несколько устройств.
4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Поместить на карантин**.
5. В открывшейся правой панели выполните следующее:
   a. В поле **Полный путь** укажите полный путь к файлу, который вы хотите поместить на карантин.
   b. В поле **Активы** выберите устройства с файлами, которые нужно переместить на карантин.

      Если на шаге 2 была выбрана вкладка **Активы**, имена устройств, для которых вы установили флажки, по умолчанию указываются в поле **Активы**. Вы можете изменить их и указать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента (и его дочерним тенантам).

Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

c. При необходимости настройте следующие параметры в соответствующих полях:

- Укажите SHA256 или хеш MD5 файла.

  Если на шаге 2 вы выбрали вкладку **Наблюдаемые объекты**, хеш будет указан. При необходимости значение можно изменить.

- Напишите описание или комментарий к действию по реагированию.

6. Нажмите на кнопку **Переместить**.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Реагирование из сведений об устройстве

Чтобы переместить файл на карантин из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство с файлом, который нужно переместить на карантин.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство с файлом, который нужно переместить на карантин.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Реагирование из телеметрии события

Чтобы переместить файл на карантин из телеметрии события при его открытии из деталей алерта или инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство с файлом, который нужно переместить на карантин.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.

     Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с файлом, который вы хотите переместить на карантин, и нажать на кнопку **Переместить на карантин**.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Поместить на карантин**.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Поместить на карантин**.

4. Выполните действия, которые описаны в пунктах 5–6 в процедуре *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Реагирование из графа расследования

> Этот параметр доступен, если граф расследования построен.

Чтобы переместить файл на карантин из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство с файлом, который нужно переместить на карантин.
2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.
3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.
4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Поместить на карантин**.
5. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.
2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.
3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Поместить на карантин**.
4. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Реагирование из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите **Поместить на карантин**.

3. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удаляется из директории устройства, на котором он находится, и перемещается на карантина на том же устройстве. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение – **Успешно**. Иначе отобразится сообщение об **ошибке** с информацией о ней.

Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Выполнение действий по реагированию Добавить правило запрета и Удалить правило запрета

Правила запрета позволяют предотвратить запуск на устройствах файлов или процессов, которые вы считаете небезопасными. Kaspersky EDR Expert идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете настроить действия по реагированию **Добавить правило запрета** и **Удалить правило запрета** для добавления и удаления правила запрета для устройства или хеша файла одним из следующих способов:

- Из деталей алерта или инцидента.
- Из сведений об устройстве.
- Из графа расследования.
- Из таблицы активов.

- Из раздела **История реагирований**.
- Из сведений о событии.

  Этот параметр доступен для действия по реагированию **Добавить правило запрета**. Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.
- Из сведений файла.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

> Чтобы выполнить действия по реагированию, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Выполнение действий по реагированию из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **ID алерта** нажмите на идентификатор алерта, содержащий требуемое устройство.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **ID инцидента** нажмите на идентификатор инцидента, в котором указано требуемое устройство.
2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с требуемым устройством.

   При необходимости вы можете выбрать несколько устройств.
4. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Управлять правилами запрета**, а затем в контекстном меню выберите действие по реагированию, которое вы хотите выполнить:
   - **Добавить правило запрета**
   - **Удалить правило запрета**
5. В открывшемся окне задайте необходимые параметры действия по реагированию, выбранного на шаге 4:
   - **Для добавления правила запрета**

     В открывшейся правой панели настройте следующие параметры:

     1. В поле **MD5 или SHA256** укажите хеш файла, который вы хотите заблокировать.

        Если вы хотите указать более одного хеша, нажмите на кнопку **Добавить хеш**.
     2. При необходимости настройте следующие параметры:
        - Измените область действия по реагированию.

По умолчанию в группе параметров **Область действия** выбран параметр **Указанные активы** и раскрывающийся список **Активы** содержит названия устройств, для которых ранее были установлены флажки.

Вы можете изменить устройства для проверки, для которых нужно добавить правило запрета, или выбрать вариант **Все активы** в группе параметров **Область действия** для добавления правила запрета для всех устройств, принадлежащих тенанту алерта или инцидента и его дочерним тенантам.

> Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

- Включите переключатель **Уведомить пользователя о блокировке запуска файла**.
- В поле **Описание** напишите описание или комментарий к действию по реагированию.

3. Нажмите на кнопку **Добавить**.

Окно закрыто.

- **Для удаления правила запрета**

В открывшейся правой панели настройте следующие параметры:

1. Выберите правило, которое вы хотите удалить:

   По умолчанию в группе параметров **Правила** выбран параметр **Заданные правила**. Если вы хотите удалить правило запрета по хешу файла, в поле **MD5 или SHA256** укажите хеш файла, который нужно удалить. Если вы хотите указать более одного хеша, нажмите на кнопку **Добавить хеш**.

   Если вы хотите удалить все правила запрета, выберите **Все правила**.

2. При необходимости настройте следующие параметры:

   - Измените область действия по реагированию.

     По умолчанию в группе параметров **Область действия** выбран параметр **Указанные активы** и раскрывающийся список **Активы** содержит названия устройств, для которых ранее были установлены флажки.

     Вы можете изменить устройства для проверки, для которых нужно удалить правила запрета, или выбрать вариант **Все активы** в группе параметров **Область действия** для удаления правил запрета для всех устройств, принадлежащих тенанту алерта или инцидента и его дочерним тенантам.

     > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - В поле **Описание** напишите описание или комментарий к действию по реагированию.

3. Нажмите на кнопку **Удалить**.

Окно закрыто.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из сведений об устройстве

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **ID алерта** нажмите на идентификатор алерта, содержащий требуемое устройство.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **ID инцидента** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотр свойств**.

4. Выполните те же действия, что описаны в пунктах 4–5 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне программы перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **ID инцидента** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. Выполните те же действия, что описаны в пунктах 4–5 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Реагирование** нажмите **Управлять правилами запрета**, а затем в контекстном меню выберите действие по реагированию, которое вы хотите выполнить.

4. В открывшейся панели настройте параметры действия по реагированию, как в пункте 5 в процедуре *Выполнение действия по реагированию из деталей алерта или инцидента*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Реагирование** выберите либо **Добавить правило запрета**, либо **Удалить правило запрета**.

3. В открывшейся панели настройте параметры действия по реагированию, как в пункте 5 в процедуре *Выполнение действия по реагированию из деталей алерта или инцидента*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из сведений о событии

> Этот параметр доступен для действия по реагированию **Добавить правило запрета**.

Чтобы выполнить действие по реагированию из сведений о событии:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

2. В открывшемся окне выберите вкладку **Подробнее** и выберите нужный хеш файла.

3. Нажмите на кнопку **Добавить правило запрета** и выберите устройство, для которого вы хотите добавить правило запрета.

   Вы также можете открыть вкладку **Наблюдаемые объекты**, установить флажок рядом с хешем файла, который вы хотите заблокировать. В раскрывающемся списке **Выбор действий по реагированию** выберите **Управление правилами предотвращения**, а затем выберите **Добавить правило запрета** или **Удалить правило запрета**.

4. Выполните те же действия, которые описаны на шаге 5 в разделе *Выполнение действий по реагированию из свойств устройства*.

   Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В открывшемся окне с информацией о событии в поле Имя устройства нажмите на имя устройства, а затем в раскрывающемся списке выберите Добавить правило запрета.

Выполните те же действия, которые описаны на шаге 5 в разделе Выполнение действий по реагированию из свойств устройства.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действия по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.

- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и кнопка **Просмотреть актив**. Вы можете нажать на кнопку, а затем в открывшемся окне перейти на вкладку **Правила запрета**, чтобы просмотреть состояние правила запрета на устройстве.

Иначе отобразится сообщение об ошибке с информацией о причине.

Если вы хотите просмотреть идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

> Если вы еще не установили на устройстве приложение Kaspersky Endpoint Security со встроенным агентом и столкнулись с ошибкой при выполнении действий по реагированию, убедитесь, что имя устройства в Kaspersky EDR Expert совпадает с именем устройства в Kaspersky Anti Targeted Attack Platform версии ниже 8.0.

Управление службами

Вы можете удаленно запускать, останавливать, приостанавливать, возобновлять или удалять службу на устройстве.

Для выполнения действия по реагированию **Управлять службами** вам потребуется:

- Одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.

Вы можете выполнить действия по реагированию одним из следующих способов:

- Из деталей алерта или инцидента.
- Из сведений об устройстве.
- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.
- Из графа расследования.

  > Этот параметр доступен, если граф расследования построен.
- Из таблицы активов.
- В разделе **История реагирований**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Реагирование из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

   Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с алертом, для которого вы хотите выполнить действие по реагированию, и нажать **Управлять службами**.

3. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Управлять службами**.

5. В открывшейся панели настройте следующие параметры в соответствующих полях:

   a. Устройства, на которых вы хотите управлять службой.

      По умолчанию в группе параметров **Область действия** выбран параметр **Указанные активы** и раскрывающийся список **Активы** содержит названия устройств, для которых вы установили флажки на шаге 3.

      Вы можете изменить устройства или выбрать вариант **Все активы** в группе параметров **Область действия** для управления службами на всех устройствах, принадлежащих тенанту алерта или инцидента и его дочерним тенантам.

      Выбрать можно только те ресурсы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   b. Имя службы.

   c. Действие, которое нужно выполнить со службой: **Изменить тип запуска**, **Запустить**, **Остановить**, **Приостановить**, **Возобновить** или **Удалить**.

      Если вы выбрали действие **Изменить тип запуска**, вам нужно выбрать значение в раскрывающемся списке **Новый тип запуска**.

Настоятельно не рекомендуется останавливать, приостанавливать, удалять служб или изменять типа запуска служб, влияющих на работу на устройстве.
Список служб, которыми не рекомендуется управлять

- AVP*
- BFE
- CertPropSvc
- CoreMessagingRegistrar
- CryptSvc
- DcomLaunch
- Dhcp
- DispBrokerDesktopSvc
- EventLog
- EventSystem
- LanmanServer
- LanmanWorkstation
- LSM
- mpssvc
- Netlogon
- Netman
- PlugPlay
- PolicyAgent
- Power
- ProfSvc
- RasMan
- RpcEptMapper
- RpcSs
- SamSs
- SCardSvr

- SecurityHealthService
- SessionEnv
- Spooler
- SstpSvc
- TermService
- UmRdpService
- UserManager
- UsoSvc
- VaultSvc
- W32Time
- WebClient
- Winmgmt
- WlanSvc
- wscsvc

d. При необходимости настройте следующие параметры:

- Укажите SHA256 или хеш MD5 файла.

  Если на шаге 2 вы выбрали вкладку **Наблюдаемые объекты**, хеш будет указан. При необходимости значение можно изменить.

- Напишите описание или комментарий к действию по реагированию.

6. Нажмите на кнопку **Запустить**.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из сведений об устройстве

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

- В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

   Откроется панель с информацией об устройстве.

4. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из телеметрии события

Чтобы выполнить реагирование из телеметрии события при его открытии из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.

3. Выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшейся панели с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Управлять службами**.

4. В открывшейся панели настройте параметры действий по реагированию, которые описаны в пункте 5 процедуры *Реагирование из деталей алерта или инцидента* и запустите действие по реагированию.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из графа расследования

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. Нажмите на кнопку **Посмотреть на графе**.

3. В открывшемся графе расследования нажмите на имя устройства, а затем в раскрывающемся списке выберите **Просмотреть свойства**.

4. В открывшейся панели со сведениями об устройстве выполните действия, которые описаны в пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Управлять службами**.

4. В открывшейся панели настройте параметры действий по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите **Управлять службами**.

3. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пункте 5 инструкции *Реагирование из деталей алерта или инцидента* и запустите действие по реагированию.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действия по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение – **Успешно**. Иначе отобразится сообщение об **ошибке** с информацией о ней.

Если вы хотите просмотреть идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Получение файлов для дальнейшего анализа

Этот раздел содержит действия по реагированию, направленные на получение доказательств нарушения безопасности для дальнейшего расследования. Вы можете получить:

- Файл
- Ключ реестра
- NTFS-метафайлы
- Данные для расследования
- Образ диска
- Дамп памяти
- Дамп памяти процесса

Для выполнения действий по реагированию вам потребуется:

- Одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.

Вы можете выполнить действия по реагированию одним из следующих способов:

- Из деталей алерта или инцидента.
- из сведений об устройстве;
- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.
- Из графа расследования.

  > Этот параметр доступен, если граф расследования построен.
- Из таблицы активов.
- Из раздела **История реагирований**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Реагирование из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.
2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Если вы хотите выполнить действие по реагированию **Ключ реестра** или **Данные для расследования**, вы можете выбрать несколько устройств.
4. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Получить**.
5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Реагирование из сведений об устройстве

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.
2. В открывшемся окне выберите вкладку **Активы**.
3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

   Откроется окно с информацией об устройстве.
4. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Получить**.
5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Реагирование из телеметрии события

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.
2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:
   - Нажмите на название нужного события и выберите устройство.
   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.
3. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Получить**.
4. В открывшемся контекстном меню выберите нужное действие по реагированию.

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите нужное действие по реагированию.

Реагирование из графа расследования

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце Идентификатор нажмите на идентификатор инцидента, содержащего устройство, для которого вы хотите выполнить реагирование.

2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

   Откроется окно с информацией об устройстве.

4. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Получить**.

5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Если вы хотите выполнить действие по реагированию Данные для расследования или Ключ реестра, вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите нужное действие по реагированию.

Реагирование из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите нужное действие по реагированию.

Получение файла

Чтобы получить файл:

1. Выберите действие по реагированию Файл.

   Откроется панель **Получить файл**.

2. В поле **Полный путь** к файлу укажите полный путь к файлу, который вы хотите получить.

3. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** измените устройство, с которого вы хотите получить файл.

   - По умолчанию поле содержит имя устройства, для которого ранее вы установили флажок. Вы можете выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента и его дочерним тенантам.

     > Выбрать можно только те ресурсы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - В поле **MD5 или SHA256** укажите хеш файла, который вы хотите получить.

   - Если вы не хотите выполнять проверку файла, выключите параметр **Проверить файл**.

     По умолчанию параметр включен. Это означает, что после получения файла он проверяется на наличие угроз.

     > При запуске действия по реагированию в плейбуке необходимо добавить этот параметр вручную, если требуется выполнить проверку полученного файла.

   - В поле **Описание** напишите описание или комментарий к действию по реагированию.

4. Нажмите на кнопку **Получить**.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия реагирования файлы сохраняются в ZIP-архиве. Пароль для файла архива – *infected*.

Просмотр результата действия по реагированию

Вы можете просмотреть и скачать архив одним из следующих способов:

- В главном меню в разделе История реагирований или на вкладке История в сведениях алерта или инцидента.
- В главном меню в разделе **Файлы** или на вкладке **Файлы** в сведениях алерта или инцидента.

Если на шаге 2 вы не выключили параметр **Проверить файл**, результат проверки файла все равно отображается. После того как вы перейдете по ссылке в столбце **Статус действия**, откроются сведения о файле на вкладке **Результат**, где вы можете просмотреть результаты проверки и при необходимости скачать файл на свое устройство.

Получение ключа реестра

Чтобы получить ключ реестра:

1. Выберите действие по реагированию Ключ реестра.

   Откроется панель **Получить ключ реестра**.

2. В поле **Относительный путь к ключу реестра** укажите путь к разделу реестра, который вы хотите получить, в одном из следующих форматов:

   - Корневой относительный путь, например:

     \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - Относительный путь с указанием полного имени раздела, например:

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - Относительный путь с аббревиатурой вместо полного имени раздела, например:

     HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

3. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** измените устройства, с которых вы хотите получить ключи реестра.

     По умолчанию поле содержит имена устройств, для которых вы ранее установили флажки. Вы можете выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента и его дочерним тенантам.

     > Выбрать можно только те ресурсы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

4. В поле **Описание** напишите описание или комментарий к действию по реагированию.

5. Нажмите на кнопку **Получить**.

   Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия по реагированию будет создан REG-файл. Этот файл содержит список ключей реестра и их значений, расположенных по указанному вами пути.

Просмотр результатов действия по реагированию

Вы можете просмотреть и скачать файл одним из следующих способов:

- В главном меню в разделе **Файлы** или на вкладке **Файлы** в сведениях алерта или инцидента.

- В главном меню в разделе История реагирований или на вкладке История в сведениях алерта или инцидента.

  После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и сгенерированный файл. Иначе отобразится сообщение об **ошибке** с информацией о причине ошибки.

  Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Получение метафайлов NTFS

> Задача **Получить NTFS-метафайлы** получает только поток данных файла по умолчанию. Альтернативные (именованные) потоки данных не поддерживаются.

Чтобы получить метафайлы NTFS:

1. Выберите действие по реагированию NTFS-метафайлы.

   Откроется панель **Получить NTFS-метафайлы**.

2. В поле **Метафайлы** установите флажок напротив метафайлов, которые вы хотите получить:

   - $MFT
   - $LogFile
   - $Boot
   - $Secure
   - $Extend/$UsnJrnl

3. В поле **Том** укажите имя диска, с которого вы хотите получить метафайлы.

   По умолчанию указано значение *%SystemDrive%*.

4. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** выберите устройство, с которого требуется получить метафайлы.

     По умолчанию поле содержит имя устройства, для которого ранее вы установили флажок. Можно выбрать устройство, которое не связано с алертом или инцидентом, но принадлежит тенанту алерта или инцидента либо его дочерним тенантам.

     > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - При необходимости в поле **Описание** напишите описание или комментарий к действию по реагированию.

5. Нажмите на кнопку **Получить**.

   Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия реагирования NTFS-метафайлы сохраняются в ZIP-архиве.

Просмотр результата действия по реагированию

Вы можете просмотреть и скачать архив одним из следующих способов:

- В главном меню в разделе **Файлы** или на вкладке **Файлы** в сведениях алерта или инцидента.

- В главном меню в разделе История реагирований или на вкладке История в сведениях алерта или инцидента.

  После перехода по ссылке в столбце **Статус действия** откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и полученные файлы. Иначе отобразится сообщение об **ошибке** с информацией о причине ошибки.

  Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Получение данных для расследования

Чтобы получить данные для расследования:

1. Выберите действие по реагированию Данные для расследования.

   Откроется панель **Получить данные для расследования**.

2. В разделе **Тип информации** установите флажки рядом с типом данных, которые требуется получить:

   - **Список процессов**. Список процессов, запущенных на устройстве.

   - **Список точек автозапуска**. Список точек автозапуска.

Список включает информацию о приложениях, добавленных в папку автозагрузки или зарегистрированных в ключах реестра Run, а также о приложениях, которые автоматически запускаются при запуске указанного устройства и входе пользователя в операционную систему на устройстве.

Список поддерживаемых точек автозапуска

Поддерживаются следующие типы точек автозапуска:

- Logon
- Shell
- Office
- Browsers
- Scheduler
- Services
- Drivers
- Cryptography
- Debuggers
- COM
- SessionManager
- Network
- LSA
- Applications
- WMI
- GroupPolicy
- DriverLog
- BootLog
- Process
- OsUpdate
- Printer
- Unspecified
- OsLoader
- EfiLoader

- **Список файлов**. Список файлов и папок, хранящихся на диске.

> Максимальное число файлов, отображаемых в списке, составляет 20 000.

3. Если вы установили флажок **Список файлов**, выполните следующие действия:

   a. Укажите область поиска файлов, выбрав одну из следующих групп параметров:

   - **Все локальные диски**. В список будут включены файлы, хранящиеся во всех папках на локальных дисках.
   - **Папка**, а затем в поле **Начальная папка** укажите путь к папке, с которой должен начинаться поиск файлов.

     В список будут включены файлы, хранящиеся в указанной папке и ее подпапках.

   b. При необходимости укажите следующие критерии поиска файлов в папках:

   - Маску файлов, которые будут включены в список файлов.
   - Параметр **Дополнительные потоки данных** для записи информации о дополнительных потоках данных в списке файлов.

     По умолчанию переключатель включен.
   - Максимальный уровень вложенности папок, в которых приложение ищет файлы.
   - В поле **Исключения** укажите путь к папке, в которой требуется запретить поиск информации о файлах.

4. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** выберите устройства, с которых требуется получить данные для расследования.

     По умолчанию поле содержит имена устройств, для которых вы ранее установили флажки. Можно выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента либо его дочерним тенантам.

     > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - В поле **Описание** напишите описание или комментарий к действию по реагированию.

5. Нажмите на кнопку **Получить**.

   Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия по реагированию выбранные данные сохраняются в защищенном паролем ZIP-архиве. Пароль для файла архива – *infected*.

Просмотр результата действия по реагированию

Вы можете просмотреть и скачать архив одним из следующих способов:

- В главном меню в разделе **Файлы** или на вкладке **Файлы** в сведениях алерта или инцидента.
- В главном меню в разделе История реагирований или на вкладке История в сведениях алерта или инцидента.

  После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и полученный файл. Иначе отобразится сообщение об **ошибке** с информацией о причине ошибки.

  Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Получение образа диска

Чтобы получить образ диска:

1. Выберите действие по реагированию Образ диска.

   Откроется панель **Получить образ диска**.

2. В поле **Путь к общему сетевому ресурсу** укажите путь к общему сетевому ресурсу в формате UNC.

3. В поле **Имя пользователя** выберите имя пользователя учетной записи, которая будет использоваться для доступа к общему сетевому ресурсу.

   Вам нужно заранее настроить учетные данные для доступа к общему сетевому ресурсу в параметрах тенантов.

4. В блоке параметров **Тип диска** выполните одно из следующих действий:

   - **Логический**, а затем в поле **Том** укажите букву диска без двоеточия и косой черты, например E или C.

     Значение по умолчанию – %SystemDrive%.

   - **Физический**, а затем в поле **Физический диск** укажите путь к диску в следующем формате:

     - Для устройства с Kaspersky Endpoint Security для Windows: \\.\PHYSICALDRIVE0, \\.\PHYSICALDRIVE1, \\.\PHYSICALDRIVE2

     - Для устройства с Kaspersky Endpoint Security для Linux: /dev/sda

5. Если вы хотите разделить файл образа диска на несколько частей, включите параметр **Разделить файл на части**, а затем укажите минимальный размер одной части сохраняемого файла в ГБ.

6. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** измените устройство, с которого вы хотите получить образ диска.

По умолчанию поле содержит имя устройства, для которого ранее вы установили флажок. Можно выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента либо его дочерним тенантам.

> Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

- В поле **Описание** напишите описание или комментарий к действию по реагированию.

7. Нажмите на кнопку **Получить**.

Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия по реагированию образ диска сохраняется в EWF-файл.

> Файлы не могут быть перезаписаны: если в папке точки назначения уже есть файл с таким именем, в имени вашего EWF-файла будет указан постфикс, например Filename-1.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и путь к файлу с образом памяти диска, находящемуся на общем сетевом ресурсе. Вы можете скопировать путь.

Иначе отобразится сообщение об **ошибке** с информацией о причине ошибки.

Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

> Вы не можете перейти к общему сетевому ресурсу непосредственно из результата действия по реагированию.

Получение дампа памяти

Чтобы получить дамп памяти, выполните следующие действия:

1. Выберите действие по реагированию Дамп памяти.

   Откроется панель **Получить дамп памяти**.

2. В поле **Путь к общему сетевому ресурсу** укажите путь к общему сетевому ресурсу в формате UNC.

3. В поле **Имя пользователя** выберите имя пользователя учетной записи, которая будет использоваться для доступа к общему сетевому ресурсу.

   > Вам нужно заранее настроить учетные данные для доступа к общему сетевому ресурсу в параметрах тенантов.

4. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** выберите устройство, с которого требуется получить дамп памяти.

     По умолчанию поле содержит имя устройства, для которого ранее вы установили флажок. Можно выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента либо его дочерним тенантам.

     > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - В поле **Описание** напишите описание или комментарий к действию по реагированию.

5. Нажмите на кнопку **Получить**.

   Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия по реагированию образ диска сохраняется в RAW-файл.

> Файлы не могут быть перезаписаны: если в папке точки назначения уже есть файл с таким именем, в имени вашего RAW-файла будет указан постфикс, например Filename-1.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и путь к файлу с дампом памяти на общем сетевом ресурсе. Вы можете скопировать путь.

Иначе отобразится сообщение об **ошибке** с информацией о причине ошибки.

Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

> Вы не можете перейти к общему сетевому ресурсу непосредственно из результата действия по реагированию.

Получение дампа памяти процесса

Чтобы получить дамп памяти процесса, выполните следующие действия:

1. Выберите действие по реагированию Дамп памяти процесса.

   Откроется панель **Получить дамп памяти процесса**.

2. В поле **Идентификатор процесса** укажите идентификатор процесса, для которого вы хотите получить дамп памяти.

3. При необходимости настройте следующие параметры:

   - В раскрывающемся списке **Активы** измените устройство, с которого вы хотите получить дамп памяти процесса.

     По умолчанию поле содержит имя устройства, для которого ранее вы установили флажок. Можно выбрать устройства, которые не связаны с алертом или инцидентом, но принадлежат тенанту алерта или инцидента либо его дочерним тенантам.

     > Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

- В поле **MD5 или SHA256** укажите хеш файла процесса, для которого требуется получить дамп памяти.
- В поле **Описание** напишите описание или комментарий к действию по реагированию.

4. Нажмите на кнопку **Получить**.

   Панель закроется. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

В результате действия по реагированию дамп памяти процесса сохранится в ZIP-архив.

Просмотр результата действия по реагированию

Вы можете просмотреть и скачать архив одним из следующих способов:

- В главном меню в разделе **Файлы** или на вкладке **Файлы** в сведениях алерта или инцидента.
- В главном меню в разделе История реагирований или на вкладке История в сведениях алерта или инцидента.

  После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение **Успешно** и защищенный паролем ZIP-архив с результатами проверки. Вы можете скачать архив на ваше устройство. Пароль для файла архива: infected.

  Иначе отобразится сообщение об ошибке с информацией о причине ошибки.

  Если вы хотите просмотреть идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Получение файлов из карантина

Для выполнения действия по реагированию вам потребуется:

- Одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.

Файл на карантине, расположенный на устройстве, можно получить из карантина для дальнейшего анализа. Полученный файл отобразится в разделе **Файлы** Консоли OSMP.

Вы можете выполнить это действие по реагированию одним из следующих способов:

- Из раздела **Карантин** главного меню.
- Из результатов действия по реагированию **Поместить на карантин**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Действие по реагированию из раздела Карантин

Чтобы выполнить действие по реагированию из раздела Карантин:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Карантин**.
2. Выполните одно из следующих действий:
   - Выберите файл, который вы хотите получить из карантина.
   - Нажмите на имя файла, который вы хотите получить из карантина.

   Откроется окно со сведениями файла.
3. Нажмите на кнопку **Получить файл** и подтвердите операцию.

   > Если вы хотите, чтобы файл проверялся на наличие угроз после его получения, вы можете нажать на кнопку **Получить и проверить**.

В случае успешного завершения операции на экране отображается соответствующее сообщение и файл, помещенный на карантин, получен с устройства. Иначе отображается сообщение об ошибке.

Реагирование из результатов действия по реагированию Поместить на карантин

Для реагирования из результатов действия по реагированию Поместить на карантин выполните действия в следующем порядке:

1. Откройте результат действия **Поместить на карантин** одним из следующих способов:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.
   - В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**. В столбце **Идентификатор** нажмите идентификатор алерта или инцидента, который включает актив или наблюдаемый объект, для которого вы выполнили действие по реагированию **Поместить на карантин**. В открывшихся деталях алерта или инцидента перейдите на вкладку **История**.
2. Для результата действия по реагированию **Поместить на карантин** в столбце **Статус действия** перейдите по ссылке **Успешно**.
3. В открывшемся окне сведений нажмите на кнопку **Получить файл** и подтвердите операцию.

   > Если вы хотите, чтобы файл проверялся на наличие угроз после его получения, вы можете нажать на кнопку **Получить и проверить**.

Просмотр результата действия по реагированию

В результаты действия по реагированию отображаются:

- В разделе **Файлы** главного меню.
- В главном меню в разделе **История реагирований**.

  После того как вы перейдете по ссылке в столбце **Статус действия**, откроются сведения о файле на вкладке **Результат**, где вы можете просмотреть и при необходимости скачать файл защищенного паролем ZIP-архива на свое устройство. Пароль для файла архива – *infected*.

  Если не удалось завершить действие по реагированию, отображается сообщение об **ошибке** с информацией о причине ошибки.

  Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Проверка устройств на наличие угроз

Чтобы предотвратить распространение угрозы на зараженном устройстве, вы можете выполнить проверку устройства на наличие угроз, выполнив одно из следующих действий:

- Поиск вредоносного ПО
- Сканирование YARA
- IOC-проверка

> Чтобы выполнить действия по реагированию, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Вы можете выполнить действия по реагированию одним из следующих способов:

- Из деталей алерта или инцидента.
- из сведений об устройстве;
- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.
- Из графа расследования.

  > Этот параметр доступен, если граф расследования построен.
- Из таблицы активов.
- Из раздела **История реагирований**.

- Из списка YARA-правил или IOC-правил.

> Этот параметр доступен для действий по реагированию Сканирование YARA и IOC-проверка.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Запуск проверки из деталей алерта или инцидента

Чтобы запустить проверку устройства из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий устройство, которое требуется проверить.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.
2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с устройством, которое требуется проверить.

   При необходимости вы можете выбрать несколько устройств.
4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Проверить**.
5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Запуск проверки из сведений об устройстве

Чтобы запустить проверку из сведений об устройстве:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий устройство, которое требуется проверить.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.
2. В открывшемся окне выберите вкладку **Активы**.
3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Проверить**.

5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Запуск проверки из графа расследования

Чтобы запустить проверку устройства из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.

2. Нажмите на кнопку **Посмотреть на графе**.

3. В открывшемся графе расследования нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Проверить**.

5. В открывшемся контекстном меню выберите нужное действие по реагированию.

Запуск проверки из телеметрии события

Чтобы выполнить проверку устройства из телеметрии события при его открытии из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку Поиск угроз, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Проверить**.

4. В открывшемся контекстном меню выберите нужное действие по реагированию.

Чтобы выполнить проверку устройства из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите нужное действие по реагированию.

Запуск проверки из таблицы активов

Чтобы запустить проверку из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите нужное действие по реагированию.

Запуск проверки из раздела История реагирований

Чтобы запустить проверку из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите нужное действие по реагированию.

Запуск проверки из списка YARA-правил или IOC-правил

Чтобы выполнить проверку устройства из списка YARA-правил или IOC-правил:

1. В главном окне приложения перейдите в раздел **Правила и службы**, затем выберите **YARA-правила** или **IOC-правила**.

   Отобразится список правил.

2. Установите один или несколько флажков рядом с устройствами, для которых вы хотите запустить проверку.

3. В панели инструментов нажмите на кнопку:

   - **Запустить сканирование YARA**, если на шаге 1 вы выбрали **YARA-правила**.
   - **Запустить IOC-проверку** если на шаге 1 вы выбрали **IOC-правила**.

4. В открывшейся панели настройте параметры проверки.

Сканирование YARA

Сканирование YARA – это поиск сигнатур вредоносной активности на устройствах с помощью файлов YARA, скачанных вручную с помощью Консоли OSMP.

Для выполнения сканирования YARA у вас должно быть:

- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.
- Хотя бы одно правило в списке YARA-правил.

Чтобы выполнить YARA-проверку, выполните следующие действия:

1. Выберите действие по реагированию Сканирование YARA.

   Откроется панель **Запустить сканирование YARA**.

2. В раскрывающемся списке **Правила** выберите одно или несколько YARA-правил.

   Вы можете ввести название правила или несколько знаков из названия правила.

   > Максимальное число правил, которые вы можете указать, – 200.

3. В раскрывающемся списке **Область проверки** выполните следующие действия:

   a. Выберите параметры и укажите из значения:

   - **Оперативная память** – для сканирования процессов, запущенных на момент выполнения реагирования.

     Этот вариант выбран по умолчанию, в группе параметров **Проверить** выбран параметр **Все процессы**.

     Если требуется выполнить сканирование отдельных процессов, в группе параметров **Проверить** выберите параметр **Заданные процессы**, а затем введите имя одного или нескольких процессов, которые необходимо проверить. Иначе будет выполнено сканирование всех процессов.

     > Приложение не проверяет процессы с низким уровнем приоритета.

   - **Точки автозапуска** – для сканирования точек автозапуска, полученных от действия по реагированию **Данные для расследования**.

Затем укажите тип проверки:

- **Быстрая проверка**. Сканируются все точки автозапуска, за исключением COM-объектов.
- **Полная проверка**. Сканируются все точки автозапуска, а также файлы, связанные с ними.

Список поддерживаемых точек автозапуска

Поддерживаются следующие типы точек автозапуска:

- Logon
- Shell
- Office
- Browsers
- Scheduler
- Services
- Drivers
- Cryptography
- Debuggers
- COM
- SessionManager
- Network
- LSA
- Applications
- WMI
- GroupPolicy
- DriverLog
- BootLog
- Process
- OsUpdate
- Printer
- Unspecified

    - OsLoader
    - EfiLoader

  - **Все локальные диски** – для выполнения сканирования файлов, хранящихся во всех папках на локальных дисках.

    > Сканирование всех локальных дисков может вызвать высокую нагрузку на устройство.

  - **Заданные директории** – для сканирования файлов, находящихся в указанной директории и всех вложенных в нее папках.

    В соответствующем поле необходимо указать полный путь к директории с подстановочным символом `*` в конце, чтобы включить поддиректории, например, `C:\Users\Administrator\Desktop\*`.

b. При необходимости в соответствующих полях укажите следующие параметры для выбранного варианта:

  - **Максимальная продолжительность проверки (в часах)**

    Значение по умолчанию – 23. По истечении указанного времени проверка останавливается, даже если некоторые правила не были применены для проверки устройств. Результат действия по реагированию содержит данные, актуальные на момент остановки проверки.

  - **Исключения**

    Укажите короткие имена процессов или маску файлов, которые вы хотите добавить в исключения из сканирования. Если на устройстве запущено несколько процессов с одинаковыми именами, приложение исключает все такие процессы из сканирования.

4. При необходимости настройте следующие параметры:

  - Укажите тенант.

    Если действие по реагированию выполнялось из списка YARA-правил и были выбраны правила, принадлежащие разным тенантам, поле **Тенант** не заполняется. Необходимо вручную указать тенант, для устройства которого требуется подвергнуть YARA-проверке.

  - Измените область действия по реагированию.

    По умолчанию в группе параметров **Область действия** выбран параметр **Указанные активы** и раскрывающийся список **Активы** содержит названия устройств, для ранее были установлены флажки. На этих устройствах будет выполняться сканирование YARA.

    Вы можете изменить устройства для проверки или выбрать вариант **Все активы** в группе параметров **Область действия** для проверки всех устройств, принадлежащих тенанту алерта или инцидента (и его дочерним тенантам).

Выбрать можно только те активы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

- В поле **Описание** напишите описание или комментарий к действию по реагированию.

5. Нажмите на кнопку **Запустить**.

   Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действия по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

В столбце **Активы** необходимо перейти по ссылке с количеством активов, для которых было запущено сканирование YARA. В открывшемся окне с выбранной вкладкой **Результат** вы можете просмотреть статус сканирования для каждого YARA-правила. Если при проверке будет найдена угроза, будет создан соответствующий алерт. Вы можете перейти к алерту из результатов выполнения действия по реагированию.

Если не удалось завершить действие по реагированию, отображается сообщение об **ошибке** с информацией о причине ошибки.

IOC-проверка

IOC-проверка – это поиск признаков целевых атак, а также зараженных и возможно зараженных объектов на устройствах с помощью IOC-файлов (индикаторов компрометации), скачанных вручную через Консоль OSMP.

Для выполнения IOC-проверки необходимо следующее:

- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.
- Хотя бы одно правило в списке IOC-правил.

Чтобы выполнить IOC-проверку, выполните следующие действия:

1. Выберите действие по реагированию IOC-проверка.

   Откроется панель **Запустить IOC-проверку**.

2. В раскрывающемся списке **Правила** выберите одно или несколько IOC-правил.

3. При необходимости настройте следующие параметры:

- Укажите тенант.

  Если действие по реагированию выполнялось из списка IOC-правил и были выбраны правила, принадлежащие разным тенантам, поле **Тенант** не заполняется. Необходимо вручную указать тенант, для устройства которого требуется подвергнуть IOC-проверке.

- Измените область действия по реагированию.

  По умолчанию в группе параметров **Область действия** выбран параметр **Указанные активы** и раскрывающийся список **Активы** содержит названия устройств, для которых ранее были установлены флажки. Это означает, что на этих устройствах будет выполняться IOC-проверка.

  Вы можете изменить устройства для проверки или выбрать вариант **Все активы** в группе параметров **Область действия** для проверки всех устройств, принадлежащих тенанту алерта или инцидента (и его дочерним тенантам).

  > Выбрать можно только те ресурсы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

- В поле **Максимальная продолжительность проверки (в часах)** укажите максимальную продолжительность проверки.

  Значение по умолчанию – 23. По истечении указанного времени проверка останавливается, даже если некоторые правила не были применены для проверки устройств. Результат действия по реагированию содержит данные, актуальные на момент остановки проверки.

- В поле **Описание** напишите описание или комментарий к действию по реагированию.

4. Нажмите на кнопку **Запустить**.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действия по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.

- На вкладке История в деталях алерта или инцидента.

В столбце **Активы** нужно перейти по ссылке с количеством активов, для которых была запущена IOC-проверка. В открывшемся окне с выбранной вкладкой **Результат** можно просмотреть статус проверки для каждого IOC-правила. Если при проверке будет найдена угроза, будет создан соответствующий алерт. Вы можете перейти к алерту из результатов выполнения действия по реагированию.

Если не удалось завершить действие по реагированию, отображается сообщение об ошибке с информацией о причине ошибки.

Удаление файла

Для выполнения действия по реагированию **Удалить файл** вам потребуется:

- Одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Установленный на ваших устройствах Kaspersky Endpoint Security со встроенным агентом.

Вы можете выполнить действия по реагированию одним из следующих способов:

- Из деталей алерта или инцидента.
- из сведений об устройстве;
- Из телеметрии события.

  Сведения о событии можно открыть из сведений алерта или инцидента либо в разделе **Поиск угроз**.
- Из графа расследования.

  > Этот параметр доступен, если граф расследования построен.
- Из таблицы активов.
- В разделе **История реагирований**.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Реагирование из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется удалить.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется удалить.
2. В открывшемся окне выберите вкладку **Активы**.

   > Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с файлом, который вы хотите удалить, и нажать **Удалить файл**.

3. Установите флажок рядом с устройством, на котором расположен файл, который нужно удалить.

   Вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Удалить файл**.

5. В открывшейся правой панели выполните следующее:

   - В поле **Полный путь** укажите полный путь к файлу, который вы хотите удалить.

   - В раскрывающемся списке **Активы** выберите устройства, на которых расположен файл.

     Если на шаге 2 была выбрана вкладка **Активы**, имена устройств, отмеченных флажками, по умолчанию указываются в поле **Активы**.

     Вы можете изменить устройства или выбрать параметр **Все активы** в блоке параметров **Область действия**, чтобы выполнить действие по реагированию для всех устройств, принадлежащих тенанту алерта или инцидента (и его дочерним тенантам).

     > Для выбора доступны только те активы, с которыми вы можете выполнить действие по реагированию.
     > Устройства отображаются следующим образом: устройства, относящиеся к алерту или инциденту, помещаются в начало раскрывающегося списка **Активы**, а затем отображаются устройства в алфавитном порядке, принадлежащие тенанту алерта или инцидента, а также дочерним тенантам.

   - При необходимости настройте следующие параметры в соответствующих полях:

     - Укажите SHA256 или хеш MD5 файла.

       > Если на шаге 2 вы выбрали вкладку **Наблюдаемые объекты**, хеш будет указан. При необходимости значение можно изменить.

     - Напишите описание или комментарий к действию по реагированию.

6. Нажмите на кнопку **Удалить**.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из сведений об устройстве

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется удалить.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется удалить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотр свойств**.

4. Выполните действия, которые описаны в пунктах 4–6 в разделе *Реагирование из деталей алерта или инцидента*.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из телеметрии события

Чтобы выполнить реагирование из телеметрии события при его открытии из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется удалить.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется удалить.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужное устройство.

3. Выполните действия, которые описаны в пунктах 4–6 в разделе *Реагирование из деталей алерта или инцидента*.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Чтобы выполнить действие по реагированию из телеметрии события при его открытии из раздела Поиск угроз:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшейся панели с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Удалить файл**.

4. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из графа расследования

Чтобы запустить проверку устройства из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется удалить.

2. Нажмите на кнопку **Посмотреть на графе**.

3. В открывшемся графе расследования нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Удалить файл**.

5. Выполните действия, которые описаны в пунктах 5–6 в разделе *Реагирование из деталей алерта или инцидента*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Действия по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Удалить файл**.

4. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите **Удалить файл**.

3. В открывшейся панели настройте параметры действия по реагированию, которые описаны в пунктах 5–6 процедуры *Реагирование из деталей алерта или инцидента*.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение – **Успешно**. Иначе отобразится сообщение об ошибке с информацией о причине.

Если вы хотите просмотреть Идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

> Если файл заблокирован другим процессом, то отобразится результат со статусом **Успешно**, при этом файл будет удален только после перезагрузки устройства. Рекомендуется проверить успешность удаления файла после перезагрузки устройства.

Реагирование с помощью Active Directory

Вы можете интегрировать Kaspersky EDR Expert со службами Active Directory, которые используются в вашей организации. Active Directory считается интегрированной с Kaspersky EDR Expert после настройки интеграции между Active Directory и KUMA.

Процесс настройки интеграции Kaspersky EDR Expert и Active Directory заключается в настройке подключений к LDAP. Вам нужно настроить подключения к LDAP отдельно для каждого тенанта.

В результате, если возникнет алерт или инцидент, вы сможете выполнить действия по реагированию в отношении связанных пользователей этого тенанта.

Вы можете выполнить действие по реагированию с помощью Active Directory одним из следующих способов:

- из деталей алерта или инцидента;
- из события телеметрии (если вы открываете его из деталей алерта);
- из графа расследования.

  Этот параметр доступен, если граф расследования построен.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действие по реагированию с помощью Active Directory, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Чтобы выполнить действие по реагированию с помощью Active Directory:

1. В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**.

   Если вы хотите выполнить действие по реагированию из телеметрии события, выберите раздел **Алерты**.

   Если вы выполняете действие по реагированию из графа расследования, выберите раздел **Инциденты**.

2. Нажмите на идентификатор нужного алерта или инцидента.

3. В открывшемся окне выполните одно из следующих действий:

   - Если вы хотите выполнить действие по реагированию с помощью деталей алерта или инцидента, выберите вкладку **Активы** и нажмите на имя пользователя.
   - Если вы хотите выполнить действие по реагированию с помощью события телеметрии, выберите вкладку **Подробнее**, а затем либо нажмите на имя требуемого события и выберите пользователя, либо нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужного пользователя.
   - Если вы хотите выполнить действие по реагированию с помощью графа расследования, нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на имя пользователя.

   В правой части экрана откроется окно **Информация об учетной записи**.

4. В раскрывающемся списке **Реагирование через Active Directory** выберите действие, которое вы хотите выполнить:

   - **Заблокировать учетную запись**

     Если учетная запись пользователя заблокирована как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

   - **Сбросить пароль**

     Если пароль учетной записи пользователя сброшен как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

- **Добавить пользователя в группу безопасности**

  В открывшемся окне в поле **Группа безопасности DN** укажите полный путь к группе безопасности, в которую вы хотите добавить пользователя. CN = Team, OU = Groups, OU = ExchangeObjects, DC = example, DC = com. Нажмите на кнопку **Добавить**. В рамках одной операции можно указать только одну группу.

  Если пользователь добавлен в группу безопасности как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

- **Удалить пользователя из группы безопасности**

  В открывшемся окне в поле **Группа безопасности DN** укажите полный путь к группе безопасности, из которой вы хотите удалить пользователя. Например, CN = Team, OU = Groups, OU = ExchangeObjects, DC = example, DC = com. Нажмите на кнопку **Удалить**. В рамках одной операции можно указать только одну группу.

  Если пользователь удален из группы безопасности как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Включение и отключение сетевой изоляции

Вы можете включить или выключить сетевую изоляцию на устройстве одним из следующих способов:

- из деталей алерта или инцидента;
- из сведений об устройстве;
- из графа расследования;
- из таблицы активов;
- из сведений о событии.

  Параметр доступен только для включения сетевой изоляции.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

> Чтобы выполнить действия по реагированию, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Для устройств с установленным приложением Kaspersky Endpoint Security со встроенным агентом статус изоляции сети отображается в сведениях об устройстве.

Устройство может иметь один из следующих статусов: *Изолировано*, *Изоляция*, *Ошибка применения изоляции*, *Не изолировано*.

Также статус сетевой изоляции отображается в таблице активов, при ее открытии на вкладке **Активы** в деталях алерта или инцидента или в разделе **Управление активами** → **Активы (Устройства).** Значения в столбце **Статус изоляции** можно отфильтровать, чтобы отобразить устройства с требуемым статусом сетевой изоляции.

Выполнение действий по реагированию из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Установите флажок рядом с требуемым устройством.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбор действий по реагированию** нажмите **Сетевая изоляция**, а затем в контекстном меню выберите действие по реагированию, которое вы хотите выполнить:

   - **Включить**

     Если вы выберете это действие по реагированию для устройства, на котором уже включена сетевая изоляция, параметры будут перезаписаны новыми значениями.

     > Перед включением сетевой изоляции убедитесь, что активы импортированы из Kaspersky Security Center: в разделе **Задачи** → **Обнаружение и реагирование** задача **Импорт активов KSC** отображается со статусом Завершено.

   - **Выключить**

     После выбора этого действия по реагированию в диалоговом окне подтверждения нажмите **Выключить**.

     Вы можете выбрать это действие по реагированию для устройств, на которых включена сетевая изоляция.

5. Если вы выбрали **Включить**, в открывшейся панели настройте следующие параметры:

   a. В раскрывающемся списке **Активы** укажите устройства, которые необходимо изолировать.

   По умолчанию отображаются устройства, для которых вы установили флажки ранее. При необходимости вы можете изменить устройства. Вы не можете выбрать устройства со следующими статусами: **Изолировано**, **В процессе изоляции**, **Ошибка применения изоляции**.

   > Выбрать можно только те устройства, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   b. Укажите период изоляции устройства и единицы измерения.

c. В поле **Описание** напишите описание или комментарий к действию по реагированию.

d. Если вы хотите добавить исключение из правила сетевой изоляции, нажмите на кнопку **Добавить исключение** и в раскрывающемся списке **Направление сетевого трафика** выберите одно из следующих значений:

- **Входящий**, а затем в соответствующих полях укажите IP-адрес устройства, который необходимо исключить из блокировки сетевого трафика, и диапазон локальных портов.
- **Исходящий**, а затем в соответствующих полях указать IP-адрес устройства, который необходимо исключить из блокировки сетевого трафика, и диапазон удаленных портов.
- **Входящий/Исходящий**, а затем укажите IP-адрес устройства, который нужно исключить из сетевой изоляции.

6. Нажмите на кнопку **Включить**.

Панель будет закрыта. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из сведений об устройстве

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.
- В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотр свойств**.

4. Выполните те же действия, что описаны в пунктах 4–6 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. Выполните те же действия, что описаны в пунктах 4–6 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   > Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите один из следующих вариантов:

   - **Включить сетевую изоляцию**, а затем в открывшейся панели настройте параметры действия по реагированию.

   - **Выключить сетевую изоляцию**, а затем в диалоговом окне подтверждения нажмите **Выключить**.

Включение сетевой изоляции из информации о событии

Чтобы включить сетевую изоляцию из сведений о событии:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Включить сетевую изоляцию**.

4. В открывшейся панели настройте параметры действия по реагированию.

Если вы еще не установили на устройстве приложение Kaspersky Endpoint Security со встроенным агентом и столкнулись с ошибкой при выполнении действий по реагированию, убедитесь, что имя устройства в Kaspersky EDR Expert совпадает с именем устройства в Kaspersky Anti Targeted Attack Platform версии ниже 8.0.

Запуск приложения

Вы можете выполнить действие по реагированию одним из следующих способов:

- из деталей алерта или инцидента;
- из сведений об устройстве;
- из графа расследования;
- из таблицы активов;
- из раздела **История реагирований**;
- из сведений о событии.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действия по реагированию, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Выполнение действия по реагированию из деталей алерта или инцидента

Чтобы выполнить действие по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.
2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с требуемым устройством.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбор действий по реагированию** выберите **Запустить**, а затем в контекстном меню нажмите **Приложение**.

5. В открывшейся правой панели выполните следующее:

   a. В поле **Полный путь** укажите полный путь к исполняемому файлу, который нужно запустить.

   b. При необходимости настройте следующие параметры:

   - Измените область действия по реагированию.

     По умолчанию в раскрывающемся списке **Область действия** выбран параметр **Указанные активы** и поле **Активы** содержит названия устройств, для которых вы ранее установили флажки. Это означает, что исполняемый файл должен быть запущен на этих устройствах.

     Вы можете изменить устройства для проверки или выбрать вариант **Все активы** в выпадающем списке **Область действия** для проверки всех устройств, принадлежащих тенанту алерта или инцидента (и его дочерним тенантам).

     > Выбрать можно только те ресурсы, с которыми можно выполнить действие по реагированию. Устройства отображаются следующим образом: устройства, связанные с алертом или инцидентом, помещаются в начало раскрывающегося списка **Активы**, а затем в алфавитном порядке отображаются устройства, принадлежащие тенанту алерта или инцидента (и его дочерним тенантам).

   - В поле **Параметры командной строки** укажите дополнительные параметры для запуска исполняемого файла, например: `/all argument`.

   - В поле **Рабочая директория** укажите рабочую директорию.

   - В поле **Описание** напишите описание или комментарий к действию по реагированию.

6. Нажмите на кнопку **Запустить**.

Панель будет закрыта. Окно закрыто. Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из свойств устройства

Чтобы выполнить действие по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотр свойств**.

4. Выполните те же действия, что описаны в пунктах 4–6 процедуры *Выполнение действия по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. Выполните те же действия, что описаны в пунктах 4–6 процедуры *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Если вы еще не установили на устройстве приложение Kaspersky Endpoint Security со встроенным агентом и столкнулись с ошибкой при выполнении действий по реагированию, убедитесь, что имя устройства в Kaspersky EDR Expert совпадает с именем устройства в Kaspersky Anti Targeted Attack Platform версии ниже 8.0.

Выполнение действий по реагированию из таблицы активов

Чтобы выполнить действие по реагированию из таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Откроется таблица активов.

2. Установите флажок рядом с устройством, для которого вы хотите выполнить действие по реагированию.

   Вы можете выбрать несколько устройств.

   Архивированные устройства выбрать невозможно.

3. В раскрывающемся списке **Выбор действий по реагированию** выберите **Приложение**.

4. В открывшейся панели настройте параметры действия по реагированию, которые описаны пунктах 4–6 процедуры *Реагирование из деталей алерта или инцидента*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из раздела История реагирований

Чтобы выполнить действие по реагированию из раздела История реагирований:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   Откроется таблица с историей реагирования на все алерты и инциденты.

2. В раскрывающемся списке **Действие по реагированию** выберите **Приложение**.

3. В открывшейся панели настройте параметры действия по реагированию, как описано на пунктах 4–6 в *разделе Выполнение действия по реагированию с помощью сведений об устройстве*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из информации о событии

Чтобы выполнить действие по реагированию из информации о событии

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.

   Откроется таблица событий.

2. Нажмите на имя события, для которого нужно открыть сведения.

3. В открывшемся окне с информацией о событии нажмите на имя устройства, а затем в раскрывающемся списке выберите **Приложение**.

4. В открывшейся панели настройте параметры действия по реагированию, как описано на пунктах 4–6 в *разделе Выполнение действия по реагированию с помощью сведений об устройстве*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр результата действия по реагированию

Вы можете просмотреть результаты выполнения действий по реагированию одним из следующих способов:

- В главном меню в разделе История реагирований.
- На вкладке История в деталях алерта или инцидента.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если действие по реагированию выполнено успешно, отобразится сообщение – **Успешно**. Иначе отобразится сообщение об ошибке с информацией о причине.

Если вы хотите просмотреть идентификатор запуска и JSON с результатом действия реагирования, перейдите на вкладку **Отладка данных**.

Просмотр истории реагирования из деталей алерта или инцидента

После выполнения действия по реагированию вы можете просмотреть историю реагирования одним из следующих способов:

- В деталях алерта или инцидента.
- В разделе История реагирования.
- В сведениях о плейбуке.
- В разделе Карантин.

  Если вы установите флажок рядом с нужным файлом и нажмете на кнопку **Просмотреть файл в истории реагирования**, вы перейдете в раздел **История реагирований**. Вы можете просмотреть действие по реагированию, в результате которого файл был перемещен в раздел **Карантин**.

Чтобы просмотреть историю действий по реагированию из деталей алерта или инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг**.
2. Откройте раздел **Алерты** или **Инциденты** и нажмите на идентификатор алерта или инцидента, для которого было выполнено действие по реагированию.
3. В открывшемся окне выберите вкладку **История** и перейдите на вкладку **История реагирований**.

   Отобразится таблица событий, содержащая следующие столбцы:

   - **Время**. Время возникновения события.
   - **Запущено**. Имя пользователя, запустившего действие по реагированию.
   - **События**. Описание события.
   - **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.

- **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **Запущено** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.
- **Плейбук**. Название плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

4. Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице, если необходимо.
5. При необходимости нажмите на значок фильтра (▽) и в открывшемся окне укажите и примените критерий фильтрации:
   - Добавьте фильтр, нажав на кнопку **Добавить фильтр**.
   - Измените фильтр, выбрав необходимые значения в следующих полях:
     - **Свойство**
     - **Условие**
     - **Значение**
   - Удалите фильтр.
   - Удалите все фильтры, нажав на кнопку **Сбросить все**.

Работа с файлами, полученными в результате действий по реагированию

Для просмотра раздела **Файлы** у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.

В разделе **Файлы** отображаются файлы, которые вы загрузили вручную и получили в результате выполнения следующих действий по реагированию: Файл, Данные для расследования, Ключ реестра, NTFS-метафайлы, Дамп памяти процесса, Получить файл из карантина.

Рекомендуется включить автоматическую ротацию файлов, чтобы самые старые файлы удалялись из раздела **Файлы** и можно было загружать новые файлы. Файлы, для которых обнаружена угроза, не удаляются. Такие файлы связаны с алертами, созданными в результате обнаружения угроз.
Вы не будете получать уведомления об удалении самых старых файлов.

Просмотр таблицы файлов

Чтобы открыть таблицу файлов, из главного меню перейдите в **Хранилища** → **Файлы**. В таблице отображаются файлы, хранящиеся в тенантах, к которым у вас есть права доступа.

В правой верхней части панели инструментов вы можете группировать, фильтровать и искать данные в таблице следующим образом:

- Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.
- Нажмите на значок поиска (🔍), в появившемся поле **Поиск** введите поисковый запрос и нажмите клавишу **ENTER**.

Таблица содержит следующие столбцы:

- **Имя или полный путь**. Если вы загрузили файл вручную, имя файла будет отображаться в столбце. Если файл получен в результате действия по реагированию, будет отображаться полный путь к файлу.
- **Размер**. Размер файла.
- **MD5**. MD5-хеш файла, если таковой имеется.
- **SHA256**. SHA256-хеш файла, если таковой имеется.
- **Когда загружен**. Дата добавления файла в хранилище **Файлы**.
- **Обновлено**. Дата обновления файла в хранилище **Файлы**.

- **Тенант**. Тенант, к которому привязан файл.

  Если в иерархии экземпляров OSMP, тенант был создан на дочернем экземпляре, в поле **Тенант** отображается значок дочернего экземпляра (🗄).

- **Источник**. Имя пользователя, который добавил файл в хранилище **Файлы**, или имя устройства, с которого файл был получен в результате действия по реагированию.

- **Способ добавления**. Метод, с помощью которого файл был добавлен в хранилище **Файлы**.

  Если файл был загружен пользователем, в столбце будет отображаться значение **Загружен пользователем**. Если файл был получен в результате действия по реагированию, будет отображаться имя соответствующего действия.

- **Статус проверки**. Результат последней проверки файла. В этом столбце могут отображаться следующие значения:

  - **Не проверено**
  - **Проверяется**
  - **Не обнаружено**
  - **Обнаружено**
  - **Ошибка**

- **Описание**. В столбце отображается информация (если таковая имеется), указанная вами в поле **Описание** при настройке параметров действия по реагированию или загрузке файла вручную.

Вы можете фильтровать данные в столбцах **Способ добавления** и **Статус проверки**, нажав на заголовок столбца и выбрав интересующий вас метод или статус из раскрывающегося списка.

Выполнение действий в таблице файлов

В левой верхней части панели инструментов вы можете выполнить следующие действия:

- Обновить данные в таблице, нажав на кнопку **Обновить**.

- Загрузить файл со своего компьютера в хранилище **Файлы**, нажав на кнопку **Загрузить**.

  При этом справа откроется панель. В поле **Тенант** нужно будет указать тенант, которому будет принадлежать файл. Затем нажмите на ссылку **Загрузка файлов** и выберите файл на своем компьютере. При необходимости вы также можете добавить комментарий или описание в поле **Описание** и включить переключатель **Проверка файлов после загрузки**, если вы хотите проверять файлы на наличие угроз.

  После того как вы нажмете на кнопку **Загрузить**, панель закроется, а загруженный файл отобразится в таблице. При загрузке большого файла или нескольких файлов вам нужно обновить таблицу, чтобы в ней отображались новые файлы. Если загрузка файла выполняется, в столбце **Имя или полный путь** отображается индикатор загрузки, а в столбце **Размер** отображается размер уже загруженного файла.

- Сохраните файлы на свое устройство. Для этого установите флажок рядом с одним или несколькими файлами в таблице, а затем нажмите на кнопку **Скачать**.

- Проверить выбранные файлы на наличие угроз с помощью следующих технологий: YARA, Sandbox и Anti-Malware Engine. Для этого установите флажок рядом с одним или несколькими файлами в таблице и нажмите на кнопку **Проверить**.

- Удалить файлы. Для этого установите флажок рядом с одним или несколькими файлами в таблице, а затем нажмите на кнопку **Удалить**.

- Перейти к списку алертов, с которыми связаны файлы. Для этого установите флажок рядом с одним или несколькими файлами в таблице, а затем нажмите на кнопку **Найти алерты**. Будут отображены алерты, которые были созданы в результате обнаружения угроз, и те, по данным которых вы запускали действия по реагированию (если файл был помещен в хранилище **Файлы** в результате действия по реагированию).

Параметр **Проверить** недоступен и хеш не рассчитывается для файлов, полученных в результате следующих действий: Данные для расследования, Ключ реестра, NTFS-метафайлы, Дамп памяти процесса.

Просмотр сведений файла

Вы можете открыть сведения файла, нажав на ссылку в столбце **Имя или полный путь** таблицы.

В панели, которая откроется справа, будут отображаться метаданные файла (например, имя или путь к файлу, размер, хеш), а также статус и результат его проверки:

- Если на проверку был отправлен архив, в деталях файла отображается информация о тех файлах в архиве, для которых была обнаружена угроза, а также хеши таких файлов и их статус в каждой технологии (Anti-Malware, Sandbox, YARA).

- Если файл не был проверен, отображается соответствующая информация.

- Если проверка файла невозможна, в сведениях файла отображаются только метаданные.

Если файл был загружен вручную и проверен на наличие угроз, в сведениях файла также можно просмотреть отчет о проверке, нажав на ссылку **Загрузить отчет** в поле **Статус проверки**.

В разделе сведений файла можно выполнить следующие действия:

- Вы можете выполнять следующие действия с помощью соответствующих кнопок на панели инструментов: проверка, загрузка и удаление файлов, поиск связанных с ними алертов, изменение описания файла, переход в историю действий по реагированию.

  Параметр **Показать в истории реагирований** недоступен для файлов, загруженных вручную. Для файла, который был получен в результате действия по реагированию, после нажатия кнопки **Показать в истории реагирований** вы перейдете в раздел **История реагирований**, где будет отображаться таблица событий с фильтрацией по файлу.

- Перейдите по ссылке с хешем MD5 или SHA256, а затем в раскрывающемся списке выберите действие, которое хотите выполнить:
  - **Создать правило запрета** для файла, в котором обнаружена угроза. После выбора этого варианта откроется панель **Добавить правило запрета**, в которой можно работать с таблицей правил запрета.
  - **Найти на Kaspersky TIP** позволит проверить хеш файла в Kaspersky Threat Intelligence Portal.
  - **Просмотреть отчет Sandbox**. Данный параметр доступен для файлов, загруженных в хранилище **Файлы** вручную и проверенных с помощью технологии Sandbox.
  - **Найти связанные алерты**. Связанными называются алерты, которые были созданы в результате обнаружения угроз, и те, по данным которых вы запускали действия по реагированию (если файл был помещен в хранилище **Файлы** в результате действия по реагированию).
  - **Найти связанные события** – при этом вы перейдете в раздел **Поиск угроз**, где будет отображаться таблица событий с фильтрацией по хешу файла.

В иерархии экземпляров OSMP файлы, загруженные и полученные в результате действий по реагированию, выполненных на дочернем экземпляре, отображаются в таблице файлов в родительском экземпляре в поле **Тенант** со следующим значком: ( ).

Работа с таблицей правил запрета

Правила запрета позволяют предотвратить запуск на устройствах файлов или процессов, которые вы считаете небезопасными. Kaspersky EDR Expert идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете управлять правилами запрета следующими способами:

- Создавать вручную, импортировать, изменять и удалять правила запрета из таблицы правил запрета, как описано в этой статье.
- Создавать и удалять правила запрета, выполняя соответствующие действия по реагированию.
- Настраивать автоматический запуск действий по реагированию при создании или изменении плейбука.

Чтобы открыть таблицу правил запрета, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.
Чтобы создать или импортировать правила запрета, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Чтобы открыть таблицу правил запрета, в главном меню перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила запрета**.

Таблица содержит следующие столбцы:

- **Имя**. Для правил запрета, созданных вручную, в столбце отображается имя, указанное в панели **Создать правило запрета**. Для импортированных правил запрета в столбце отображается хеш файла.
- **Хеш**. MD5- или SHA256-хеш файла, который нужно заблокировать.
- **Тенант-владелец**. Тенант, которому принадлежит правило запрета.

  Если в режиме распределенного решения тенант был создан на резервном узле, в поле **Тенант** отображается значок резервного узла (🖴).
- **Активы**. Устройства, для которых применяется правило запрета. В столбце отображается либо количество устройств, либо значение **Все активы тенанта**.
- **Создано**. Дата и время создания или импорта правила запрета.
- **Создал**. Пользователь, создавший или импортировавший правило запрета.
- **Обновлено**. Дата и время последнего изменения параметров правила запрета.
- **Обновил**. Пользователь, который последним изменил параметры правила запрета.
- **Статус правила**. Если правило запрета включено, в этом столбце для правила отображается значение **Включено**. В противном случае отображается значение **Выключено**.
- **Уведомлять о блокировке файла**. Если при создании или изменении правила запрета вы выключили уведомление о блокировке файла, в столбце отображается значение **Нет**. В противном случае отображается значение **Да**.

В таблице вы можете выполнить следующие действия:

- Создать или импортировать правило запрета.
- Удалите правило запрета, установив флажок рядом с именем нужного правила и нажав на кнопку **Удалить** в панели инструментов. Вы также можете удалить сразу все правила.
- Чтобы включить или отключить правило запрета, установите флажок рядом с названием нужного правила, нажмите на кнопку **Изменить статус**, а затем выберите **Включить** или **Выключить**. Вы также можете включать и выключать сразу все правила.
- Просмотрите и измените параметры правила запрета, нажав на имя правила в таблице.

  Откроется панель **Изменить правило запрета** на вкладке **Подробнее**. Вы можете изменить параметры правила запрета. Параметры совпадают с теми, которые были указаны создании правила запрета из таблицы правил. Также вы можете нажать на кнопку **Перейти в Поиск угроз**, чтобы просмотреть события, полученные при срабатывании правила запрета.

  На вкладке **Журнал изменений** вы можете просмотреть все изменения правила запрета одним из следующих способов: вручную из таблицы правил запрета, выполнить действие по реагированию или запустить плейбук.

Чтобы применить действие ко всем правилам сразу:

1. Установите флажок рядом со столбцом **Имя**.
2. В раскрывающемся списке выберите один из объектов:
   - **Выбрать все** – если вы хотите выполнить действие для всех правил в таблице.
   - **Выбрать все на текущей странице** – если вы хотите выполнить действие для всех правил на текущей странице.
3. При необходимости вы можете исключить одно или несколько правил из области действия, сняв флажки рядом с названиями правил.
4. В панели инструментов нажмите на нужную кнопку в зависимости от того, какое действие вы хотите выполнить: **Удалить** или **Изменить статус** (включить или выключить правила).

Действие будет применено ко всем выбранным вами правилам.

Создание правила запрета

Чтобы создать правило запрета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила запрета**.

   Отобразится таблица правил запрета.
2. В панели инструментов нажмите на кнопку **Создать**.
3. В открывшейся панели **Создать правило запрета** настройте нужные параметры:

   a. В поле **Тенант-владелец** укажите тенант, которому будет принадлежать правило запрета.

   > После сохранения параметров правила запрета изменить значение в поле **Тенант-владелец** невозможно. Если вы хотите сменить тенант, вам нужно удалить правило запрета, создать другое правило и указать нужное значение в поле **Тенант-владелец**.

   b. В поле **MD5 или SHA256** укажите хеш файла, который вы хотите заблокировать.

   Если вы хотите указать более одного хеша, нажмите на кнопку **Добавить хеш**.

   > Приложение проверяет наличие хеша тенанта в списке блокируемых хешей файлов. Вы не можете указать такие хеши при создании правила запрета.

   c. При необходимости настройте следующие параметры:

   - Измените область действия правила запрета.

     По умолчанию в группе параметров **Область применения** выбран параметр **Все активы**. Это означает, что правило запрета применяется ко всем устройствам. Вы можете выбрать параметр **Указанные активы**, а затем в отобразившемся поле **Активы** указать одно или несколько устройств, к которым вы хотите применить правило запрета.

Если вы указали устройства, к которым вы хотите применить правило запрета, а затем устройство будет удалено, такое устройство также будет удалено из правила запрета и соответствующая информация отобразится на вкладке **Журнал изменений** сведений правила запрета.

- В поле **Имя правила** укажите название правила запрета. Если вы не укажете имя, поле будет пустым.
- Если вы не хотите получать уведомления о блокировке файлов, в поле **Уведомить пользователя о блокировке запуска файла** выключите переключатель.

  По умолчанию параметр включен.
- Если вы не хотите применить правило запрета, в поле **Статус** выключите переключатель.

  Если вы хотите создать правило запрета со статусом **Выключено**, вам нужно сначала настроить другие параметры. В противном случае не удастся сохранить правило.

d. Нажмите на кнопку **Создать**.

Панель будет закрыта, правило запрета отобразится в списке правил.

Импорт правил запрета

Чтобы импортировать правило запрета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила запрета**.

   Отобразится таблица правил запрета.

2. В панели инструментов нажмите на кнопку **Импортировать**.

   Правила запрета, импортированные из файла, будут применены к активам, которые принадлежат тенанту, включая дочерние тенанты.

3. В открывшейся панели **Импортировать правила запрета** настройте нужные параметры:

   a. Выберите файл CSV на вашем устройстве.

   Вы можете добавить только один файл CSV, содержащий хеши. Число хешей равно числу создаваемых правил запрета. Максимальный размер файла не должен превышать 15 МБ.

   b. В раскрывающемся списке укажите, к какому тенанту будут применяться правила запрета.

   По умолчанию отображается тенант, к которому у вас есть права доступа. При необходимости вы можете изменить значение.

   Если у вас есть права доступа к нескольким тенантам, вам нужно будет указать тенант самостоятельно.

   c. Нажмите на кнопку **Импортировать**.

Панель будет закрыта, а импортированное правило запрета отобразится в таблице правил.

Работа с таблицей IOC-правил

Kaspersky EDR Expert выполняет проверку устройств на наличие индикаторов компрометации (IOC). Несколько IOC объединяются в структурированное описание в IOC-файле. При импорте IOC-правила Kaspersky EDR Expert извлекает структурированное описание из IOC-файла и создает правило на основе описания. После срабатывания IOC-правила формируется алерт IOC.

Просмотр таблицы IOC-правил

Для просмотра таблицы IOC-правил необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.

Чтобы открыть таблицу IOC-правил, в главном меню перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **IOC-правила**. В таблице отображаются IOC-правила, хранящиеся в тенантах, к которым у вас есть права доступа.

Вы можете группировать, фильтровать и выполнять поиск данных в таблице следующим образом:

- Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.
- Нажмите на значок поиска (🔍), в появившемся поле **Поиск** введите поисковый запрос и нажмите клавишу **ENTER**.

Таблица содержит следующие столбцы:

- **Имя**. Название IOC-правила.
- **Создано**. Дата и время создания IOC-правила.
- **Создал**. Пользователь, создавший IOC-правило.
- **Обновлено**. Дата обновления IOC-правила.
- **Обновил**. Пользователь, который последним изменил параметры IOC-правила.
- **Важность**. Уровень важности IOC-правила: **Низкий**, **Средний** или **Высокий**.
- **Тенант-владелец**. Тенант, которому принадлежит IOC-правило.

  Если в режиме распределенного решения тенант был создан на дочернем экземпляре, в поле **Тенант** отображается значок дочернего экземпляра ( ).
- **Проверка по расписанию**. Статус проверки по расписанию: **Включено** или **Выключено**. Чтобы изменить статус, переведите переключатель в положение **Включено** или **Выключено**.

Выполнение действий в таблице IOC-правил

В левой верхней части панели инструментов вы можете выполнить следующие действия:

- Обновить данные в таблице, нажав на кнопку **Обновить**.
- Чтобы импортировать IOC-правила из файлов, содержащих IOC-правила, **нажмите кнопку Импортировать**.

  Для этого необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик SOC, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Сохраните IOC-правила на свой компьютер. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Экспортировать**.
- Удаление IOC-правил. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Удалить**. Вы также можете удалить сразу все правила.
- Выполнение действия по реагированию IOC-проверка. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Запустить IOC-проверку**. Вы также можете выполнить действие по реагированию сразу для всех правил.

  Для выполнения действий необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Включение или выключение проверки по расписанию для выбранных IOC-правил. Для этого установите флажок рядом с одним или несколькими правилами в таблице, нажмите кнопку **Проверка по расписанию**, затем в раскрывающемся меню выберите **Включить** или **Выключить**. Вы также можете включить или выключить проверку сразу для всех правил.

  Проверка по расписанию требует настройки.

Чтобы применить действие ко всем правилам сразу:

1. Установите флажок рядом со столбцом **Имя**.
2. В раскрывающемся списке выберите один из объектов:
   - **Выбрать все** – если вы хотите выполнить действие для всех правил в таблице.
   - **Выбрать все на текущей странице** – если вы хотите выполнить действие для всех правил на текущей странице.

3. При необходимости вы можете исключить одно или несколько правил из области действия, сняв флажки рядом с названиями правил.

4. В панели инструментов нажмите на нужную кнопку в зависимости от того, какое действие вы хотите выполнить: **Удалить**, включить или выключить **Проверка по расписанию**.

Действие будет применено ко всем выбранным вами правилам.

Если в иерархии экземпляров OSMP в дочернем экземпляре вы включаете, выключаете или удаляете все правила сразу, а выборка содержит правила родительского экземпляра, действие не будет применено к этим правилам.
Если вы нажмете **Выбрать все** → **Проверка по расписанию** или **Выбрать все** → **Удалить**, действие будет применено только к правилам дочернего экземпляра.
Если вы нажмете **Выбрать все на текущей странице**, кнопки **Проверка по расписанию** и **Удалить** выключены.

Просмотр сведений об IOC-правиле

Чтобы открыть сведения о файле, нажмите на ссылку в столбце **Имя** таблицы.

В открывшейся панели отображаются сведения об IOC-правиле в соответствующих полях: имя правила; тенант, которому принадлежит правило; важность правила; статус проверки по расписанию (включено или выключено); условие срабатывания правила.

В разделе сведений можно выполнить следующие действия:

- Сохранить IOC-правило на свой компьютер нажатием на кнопку **Экспортировать**.
- Выполнение IOC-проверки нажатием на кнопку **Запустить IOC-проверку**.
- Переход к списку алертов, с которыми связано IOC-правило, нажатием на кнопку **Найти алерты**.

  Отображаются алерты, в которых сработало данное IOC-правило. Если таких алертов нет, отображаются все IOC-алерты.

Работа с таблицей YARA-правил

YARA-правила – это описания сигнатур целевых атак и вторжений в ИТ-инфраструктуру организации. Kaspersky EDR Expert проверяет объекты в соответствии с этими правилами.

Просмотр таблицы YARA-правил

Для просмотра таблицы YARA-правил необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.

Чтобы открыть таблицу YARA-правил, в главном меню перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **YARA-правила**.

В таблице отображаются YARA-правила, хранящиеся в тенантах, к которым у вас есть права доступа.

Вы можете группировать, фильтровать и выполнять поиск данных в таблице следующим образом:

- Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации (▽), укажите и примените критерий фильтрации в открывшемся меню.
- Нажмите на значок поиска (🔍), в появившемся поле **Поиск** введите поисковый запрос и нажмите клавишу **ENTER**.

Таблица содержит следующие столбцы:

- **Имя**. Имя YARA-правила.
- **Создано**. Дата и время создания YARA-правила.
- **Создал**. Пользователь, создавший YARA-правило.
- **Обновлено**. Дата обновления YARA-правила.
- **Обновил**. Пользователь, который последним изменил параметры YARA-правила.
- **Важность**. Уровень важности YARA-правила: **Низкий**, **Средний** или **Высокий**.
- **Тенант-владелец**. Тенант, которому принадлежит YARA-правило.

  Если в режиме распределенного решения тенант был создан на дочернем экземпляре, в поле **Тенант** отображается значок дочернего экземпляра (🗄).
- **Проверка файла**. Статус сканирования YARA: **Включено** или **Выключено**. Чтобы изменить статус, переведите переключатель в положение **Включено** или **Выключено**.
- **Описание**. Описание или комментарий к YARA-правилу.

Выполнение действий в таблице YARA-правил

В левой верхней части панели инструментов вы можете выполнить следующие действия:

- Обновить данные в таблице, нажав на кнопку **Обновить**.
- Чтобы импортировать YARA-правила из файлов, содержащих YARA-правила, нажмите кнопку **Импортировать**.

  Для импорта YARA-правил необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик SOC, Аналитик 1-го уровня, Аналитик 2-го уровня.
- Сохраните YARA-правила на свое устройство. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Экспортировать**.

- Удалите YARA-правила. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Удалить**. Вы также можете удалить сразу все правила.

- Выполните действие по реагированию Сканирование YARA. Для этого установите флажок рядом с одним или несколькими правилами в таблице, а затем нажмите на кнопку **Запустить сканирование YARA**. Вы также можете выполнить действие по реагированию сразу для всех правил.

  Для выполнения действий необходима одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

- Включение или выключение проверки по расписанию для выбранных YARA-правил. Для этого установите флажок рядом с одним или несколькими правилами в таблице, нажмите кнопку **Проверка файла**, затем в раскрывающемся меню выберите **Включить** или **Выключить**. Вы также можете включить или выключить проверку сразу для всех правил.

Чтобы применить действие ко всем правилам сразу:

1. Установите флажок рядом со столбцом **Имя**.

2. В раскрывающемся списке выберите один из объектов:

   - **Выбрать все** – если вы хотите выполнить действие для всех правил в таблице.

   - **Выбрать все на текущей странице** – если вы хотите выполнить действие для всех правил на текущей странице.

3. При необходимости вы можете исключить одно или несколько правил из области действия, сняв флажки рядом с названиями правил.

4. В панели инструментов нажмите на нужную кнопку в зависимости от того, какое действие вы хотите выполнить: **Удалить**, включить или выключить **Проверка файла**.

Действие будет применено ко всем выбранным вами правилам.

Если вы хотите включить или выключить все правила одновременно, а выборка содержит правила, принадлежащие субтенантам:

- При нажатии на кнопку **Выбрать все**, статус изменится только у правил, принадлежащих корневому тенанту.

- Если нажать на кнопку **Выбрать все на текущей странице**, кнопка **Проверка файла** неактивна.

В иерархии экземпляров OSMP применение действия сразу ко всем правилам требует учета определенных условий.

Нажмите здесь, чтобы просмотреть условия

Включение и выключение всех правил сразу

В родительском экземпляре

- Если вы нажмете на кнопку **Выбрать все**, а выборка будет содержать правила, принадлежащие субтенантам родительского или дочернего экземпляра, действие не будет применено к этим правилам.

  Для обоих экземпляров будут включены или выключены только правила, принадлежащие корневому тенанту.

- Если вы нажмете на кнопку **Выбрать все на текущей странице**, а выборка содержит правила, принадлежащие субтенантам родительского или дочернего экземпляра, кнопка **Проверка файла** будет неактивна.

В дочернем экземпляре

- Если вы нажмете на кнопку **Выбрать все**, а выборка будет содержать правила, принадлежащие дочерним тенантам, или какие-либо правила родительского экземпляра, действие будет применено только к правилам дочернего экземпляра, принадлежащим корневому тенанту.

- Если вы нажмете на кнопку **Выбрать все на текущей странице**, а выборка содержит правила, принадлежащие субтенантам, или какие-либо правила родительского экземпляра, кнопка **Проверка файла** будет неактивна.

Удаление сразу всех правил

В родительском экземпляре,

вы можете удалить любые правила, принадлежащие любым тенантам родительского и дочернего экземпляров.

В дочернем экземпляре:

- Если вы нажмете на кнопку **Выбрать все**, а выборка содержит правила родительского экземпляра, эти правила не будут удалены.

- Если вы нажмете на кнопку **Выбрать все на текущей странице**, а выборка содержит правила родительского экземпляра, кнопка **Удалить** будет неактивна.

Просмотр сведений об YARA-правиле

Вы можете открыть сведения о YARA-правиле, нажмите на ссылку в столбце **Имя** таблицы.

В открывшейся панели информация о YARA-правиле отображается в соответствующих полях: имя правила, название тенанта, которому принадлежит правило, важность правила, статус проверки (включено или выключено), описание правила и условие, при котором оно срабатывает.

В разделе сведений можно выполнить следующие действия:

- Сохранить YARA-правило на свое устройство нажатием на кнопку **Экспортировать**.
- Выполнить сканирование YARA нажатием на кнопку **Запустить сканирование YARA**.
- Переход к списку алертов, с которыми связано YARA-правило, нажатием на кнопку **Найти алерты**.

  Отображаются алерты, в которых сработало данное YARA-правило. Если таких алертов нет, отображаются все YARA-алерты.

Плейбуки

Kaspersky EDR Expert использует плейбуки, которые позволяют автоматизировать рабочие процессы и сократить время, необходимое для обработки алертов и инцидентов.

Плейбуки реагируют на алерты или инциденты в соответствии с заданным *алгоритмом*. Плейбук запускает алгоритм, включающий в себя последовательность действий по реагированию, которые помогают анализировать и обрабатывать алерты или инциденты. Вы можете запустить плейбук вручную или настроить автоматический запуск нужного плейбука.

Автоматический запуск плейбуков выполняется в соответствии с *триггером*, который вы настраиваете при создании плейбука. Триггер определяет условия, которым должен соответствовать алерт или инцидент для автоматического запуска этого плейбука.

Область действия одного плейбука ограничена только алертами или только инцидентами.

Плейбуки не могут быть запущены автоматически для дочерних инцидентов. Для дочерних инцидентов вы можете запустить плейбук только вручную. Перед запуском плейбука вам нужно выбрать активы и наблюдаемые объекты, для которых должен быть запущен плейбук. Обратите внимание, что плейбук может быть запущен только для объектов, которые принадлежат тенанту алерта или инцидента.

Обратите внимание, что плейбук может принадлежать только одному тенанту и он автоматически наследуется всеми дочерними тенантами родительского тенанта, включая дочерние тенанты, которые будут добавлены после создания плейбука. Вы можете выключить наследование плейбука дочерними тенантами при создании или изменении плейбука.

В Kaspersky EDR Expert есть два типа плейбуков:

- Предустановленные плейбуки

  Предустановленные плейбуки созданы экспертами "Лаборатории Касперского". Эти плейбуки отмечены префиксом [KL] в названии и не могут быть изменены или удалены.

  По умолчанию предустановленные плейбуки работают в режиме **Обучение**. Дополнительные сведения см. в разделе Предустановленные плейбуки.

- Пользовательские плейбуки

  Вы можете сами создавать и настраивать плейбуки. При создании пользовательского плейбука нужно указать область действия плейбука (алерт или инцидент), триггер для автоматического запуска плейбука и алгоритм реагирования на угрозы. Для получения подробной информации о создании плейбука см. раздел Создание плейбуков.

Вы можете использовать XDR REST API для импорта и экспорта плейбуков для определенного тенанта.

Режимы работы

Вы можете настроить как автоматический, так и ручной запуск плейбуков. Способ запуска плейбука зависит от выбранного режима работы.

Существуют следующие типы режимов работы:

- **Автоматический**. Плейбук в этом режиме работы автоматически запускается при обнаружении соответствующих алертов или инцидентов.
- **Обучение**. Плейбук в этом режиме работы запрашивает разрешение пользователя на запуск при обнаружении соответствующих алертов или инцидентов.
- **Ручной**. Плейбук в этом режиме работы можно запустить только вручную.

Роли пользователей.

Вы предоставляете пользователю права на управление плейбуками, назначая пользователям роли.

В таблице ниже представлены права доступа для управления плейбуками и выполнения действий пользователя.

Роль пользователя	Права пользователей				
	Чтение.	Запись.	Удалить	Выполнение.	Подтверждение действия по реагированию
Главный администратор	✓	✓	✓	✓	✓
Администратор SOC	✓	✓	✓	—	—
Младший аналитик	✓	—	—	—	—
Аналитик 1-го уровня	✓	—	—	✓	—
Аналитик 2-го уровня	✓	✓	✓	✓	—
Менеджер SOC	✓	—	—	—	—
Подтверждающий	✓	—	—	—	✓
Аудитор	✓	—	—	—	—
Администратор тенанта	✓	✓	✓	✓	✓

Действия по реагированию, доступные в плейбуках

В Kaspersky EDR Expert можно включить в плейбук следующие действия:

- Получить файл
- Собрать форензику

- Получить ключ реестра
- Получить метафайлы NTFS
- Получить дамп памяти процесса
- Получить образ диска
- Получить дамп памяти
- Завершить процесс
- Запустить YARA-проверку
- Управлять службами
- Выполнить приложение
- Удалить файл
- Поместить файл на карантин
- Удалить файл из карантина
- Восстановить файл из карантина
- Изолировать хост
- Создать правило запрета
- Удалить правило запрета
- Запустить IOC-проверку

Просмотр таблицы плейбуков

Таблица плейбуков отображается в разделе **Мониторинг** → **Плейбуки**. По умолчанию в таблице отображаются плейбуки, относящиеся ко всем тенантам, к которым у вас есть права доступа.

> В таблице плейбуков отображаются все существующие плейбуки, за исключением плейбуков в статусе **Удалено**.

Чтобы настроить таблицу плейбуков, выполните одно из следующих действий:

- Примените фильтр для тенантов:
  a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.
  b. Откроется список тенантов.
  c. Установите флажки рядом с требуемыми тенантами.

- Отфильтруйте данные таблицы плейбуков:

  a. Нажмите на значок фильтра ( ).

  b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.

- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица плейбуков настроена и отображает нужные вам данные.

Таблица плейбуков содержит следующую информацию:

- **Название**. Название пользовательских или предустановленных плейбуков.

  > Предустановленные плейбуки отмечены префиксом [KL] в названии и не могут быть изменены или удалены.

- **Статус**. Статус плейбука. Возможные значения:

  - **Активный**. Плейбук создан и готов к использованию (установлены все необходимые веб-плагины).

  - **Черновик**. Плейбук создан и сохранен как черновик. Такой плейбук невозможно запустить, но он доступен для просмотра, изменения, настройки и удаления в тенанте, которому он принадлежит.

  - **Удалено**. Плейбук удален. По умолчанию плейбуки с этим статусом не отображаются в таблице. Если вы хотите просмотреть их, нажмите на столбец **Статус** и в раскрывающемся списке выберите **Удалено**.

    > Только активные и недоступные плейбуки имеют статус **Удалено** после удаления. Плейбуки со статусом **Черновик** удаляются навсегда и не отображаются в таблице плейбуков.

  - **Недоступно**. Алгоритм плейбука использует недоступный веб-плагин или содержит действия по реагированию, которые не предоставляются вашей лицензией.

- **Режим работы**. Режим работы плейбука, определяющий способ запуска плейбука. Подробнее о режимах работы см. в разделе Плейбуки.

- **Теги**. Теги, которые назначены плейбуку. Вы можете фильтровать плейбуки, используя назначенные теги.

- **Действия**. Действия, запускаемые в плейбуках.

- **Запуски**. Общее количество запусков плейбука.

- **Изменена**. Дата и время последнего изменения плейбука.

- **Создана**. Дата и время создания плейбука.

- **Родительский тенант**. Имя тенанта, которому принадлежит плейбук.

- **Описание.** Описание плейбука или комментарий. По умолчанию этот столбец скрыт.

- **Область действия**. Область действия плейбука. Возможные значения: **Алерт** или **Инцидент**.

- **Создал**. Имя пользователя, который создал плейбук. По умолчанию этот столбец скрыт.
- **Обновил**. Имя пользователя, который изменил плейбук. По умолчанию этот столбец скрыт.

Создание плейбуков

Вы можете создать плейбук для автоматизации анализа угроз и реагирования на них.

> Чтобы создать плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Kaspersky EDR Expert также позволяет создать плейбук, соответствующий вашим потребностям, на основе существующего. Подробную информацию см. в разделе Настройка плейбуков.

Чтобы создать плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. Нажмите на кнопку **Создать**.

   Откроется окно **Создать плейбук**, в котором слева будет рабочая область визуального редактора, а справа – панель **Параметры плейбука**. Визуальный редактор позволяет вам создавать и отображать поток выполнения плейбука, а также отображать взаимосвязь между шагами, участвующими в создании плейбука.

   > На основе действий, которые вы выполняете в визуальном редакторе, формируется DSL-схема алгоритма плейбука. Изменения, вносимые вами в рабочей области визуального редактора, отображаются в коде, и наоборот. При необходимости вы можете открыть редактор кода, нажав на кнопку **Показать код** в панели инструментов.

3. В разделе **Параметры плейбука** укажите следующие параметры:
   - В поле **Тенант и наследование** выберите родительский тенант и дочерние тенанты, для которых нужно запустить плейбук.

     > Все дочерние тенанты выбранного родительского тенанта автоматически унаследуют этот плейбук. Чтобы выключить наследование плейбука, снимите флажок рядом с нужным дочерним тенантом. Наследование плейбука будет выключено для этого тенанта, а также для его субтенантов, при их наличии.
     > Если вы выберете дочерний тенант, его субтенанты будут выбраны автоматически.

   - В поле **Название** введите название плейбука.

     Обратите внимание, что название плейбука должно быть уникальным в рамках тенанта и не может быть длиннее 255 символов.

   - В списке **Область действия** выберите следующие параметры:
     - **Алерт**. Плейбук будет запускаться только для алертов. По умолчанию этот вариант выбран.
     - **Инцидент**. Плейбук будет запускаться только для инцидентов.

- В списке **Режим работы** выберите следующие параметры:

  - **Автоматический**. Плейбук в этом режиме работы автоматически запускается при обнаружении соответствующих алертов или инцидентов.

  - **Обучение**. Плейбук в этом режиме работы запрашивает разрешение пользователя на запуск при обнаружении соответствующих алертов или инцидентов.

  - **Ручной**. Плейбук в этом режиме работы можно запустить только вручную.

- При необходимости в поле **Теги** укажите до 30 тегов. Вы можете фильтровать плейбуки, используя назначенные теги.

  Максимальная длина тега составляет 50 символов.

- При необходимости в поле **Описание** введите описание плейбука или комментарий.

- В раскрывающемся списке **При одновременном запуске нескольких экземпляров плейбука** выберите действие, которое следует выполнить, если одновременно запускаются два или более экземпляров плейбуков:

  - **Добавить экземпляры плейбука в очередь**. Новый экземпляр плейбука будет запущен после завершения текущего. По умолчанию выбрано это действие.

  - **Завершить текущее выполнение и запустить новый экземпляр**. Выполнение текущего экземпляра плейбука будет прекращено. После этого запускается новый экземпляр плейбука.

  - **Не запускать новые экземпляры плейбука**. Новый экземпляр плейбука не будет запущен. Выполнение текущего экземпляра плейбука будет продолжено.

  > Раскрывающийся список **При одновременном запуске нескольких экземпляров плейбука** отображается только в том случае, если выбран режим работы **Автоматический**.

- По умолчанию плейбук запускается только для новых алертов или инцидентов, соответствующих триггеру.

  Если вы хотите запустить новый плейбук для существующих алертов или инцидентов, соответствующих триггеру, установите флажок **Запустите плейбук для всех совпадающих алертов или инцидентов. Обратите внимание, что система может быть перегружена**.

- При необходимости в разделе **Дополнительные параметры** укажите следующие параметры плейбука:

  - **Время ожидания плейбука** – максимальное время выполнения плейбука. По умолчанию указано значение 24h. Максимальное значение – 48h.

    Если вы хотите создать политики, которые будут в дальнейшем применяться в действиях по реагированию, включите переключатель **Используйте политики времени ожидания для действия по реагированию** и добавьте политики.

    > После выключения переключателя добавленные политики будут удалены.

  - **Вход** – выражение jq для изменения входных данных перед выполнением плейбука.

- **Выход** – выражение jq для изменения выходные данных после выполнения плейбука.
- **Изменить способ** – способ изменения выходных данных. Выберите, следует ли объединить текущие и новые данные или перезаписать текущие данные новыми данными, выбрав параметр **Объединить** или **Перезаписать**.

Остальные дополнительные параметры предустановлены и не могут быть изменены:

- **Версия плейбука** – версия плейбука. Может потребоваться более точное определение плейбука в телеметрии.
- **Версия DSL** – версия DSL-схемы.
- **Версия действия** – версия схемы действий по реагированию с описанием входных параметров функции реагирования.

4. В рабочей области визуального редактора настройте триггер и алгоритм плейбука. Нажмите на шаг **Триггер** и в открывшейся панели свойств триггера укажите условие автоматического запуска плейбука.

   > Если вы выберете режим работы **Ручной**, параметры триггера будут недоступны.

   Чтобы описать условие срабатывания триггера, используйте выражения jq. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

   В зависимости от того, какой параметр вы выбрали в списке **Область действия** при создании или изменении плейбука, используется модель данных алерта или модель данных инцидента.

   Например, чтобы отфильтровать алерты или инциденты по уровню важности, укажите следующее выражение:

   ```
   .Severity == "critical"
   ```

   Вы также можете указать сложные выражения для фильтрации алертов или инцидентов.

   Например, чтобы отфильтровать критические алерты или инциденты по имени правила, укажите следующее выражение:

   ```
   (.Severity == "critical") and (.Rules[] |.Name | contains("Rule_1"))
   ```

   где `Rules [] | .Name` это имя сработавшего правила.

   > Проверка выражений jq настроена. Если вы укажете неверное выражение при настройке плейбука в триггере, ошибка будет отмечена красным цветом. Если вы хотите просмотреть подробную информацию, наведите курсор мыши на ошибку.

5. Если вы хотите просмотреть алерты или инциденты, соответствующие триггеру плейбука, в разделе **Сопоставление триггеров** нажмите на кнопку **Найти**. По умолчанию отображаются 10 последних измененных алертов и инцидентов. Если вы хотите изменить значение, откройте раскрывающийся список и выберите нужное значение.

   Также можно запросить полный список алертов или инцидентов. Для этого в разделе **Триггер** введите `true` и нажмите на кнопку **Найти**.

   Отобразится полный список алертов или инцидентов.

6. Укажите шаги алгоритма плейбука.

   Алгоритм можно скопировать из другого плейбука. Для этого в панели инструментов нажмите на кнопку **Копировать алгоритм**, в открывшемся окне выберите плейбук, из которого нужно скопировать алгоритм, и нажмите на кнопку **OK**.

Проверка выражений jq и синтаксиса JSON настроена. Если вы укажете неверное выражение при настройке плейбука в алгоритме, ошибка будет отмечена красным цветом. Если вы хотите просмотреть подробную информацию, наведите курсор мыши на ошибку.

Чтобы добавить шаг алгоритма, выполните следующие действия:

a. Наведите курсор мыши на шаг, от которого необходимо построить связь с новым шагом.

   Если вы добавляете шаг в первый раз, вы можете навести курсор мыши только на шаг **Триггер**.

b. Нажмите и удерживайте значок белой точки (○), который отображается, а затем начните рисовать стрелку.

c. Отпустите курсор мыши и в открывшемся меню выберите шаг.

   Выбранный шаг отобразится в визуальном редакторе.

d. Нажмите на шаг, чтобы настроить его параметры. Подробные сведения приведены в разделе Настройка шагов выполнения плейбука в визуальном редакторе.

Также вы можете нажать правой кнопкой мыши в любой части рабочей области визуального редактора, чтобы вызвать меню, а затем выбрать шаг, который вы хотите добавить. В этом случае после добавления шага необходимо выстроить связи, нарисовав стрелки между шагами. Если связи не выстроены, вы можете сохранить плейбук только как черновик.

Если шаги алгоритма не добавлены, вы можете сохранить плейбук только как черновик.

7. Сохраните плейбук одним из следующих способов:

- Нажав на кнопку **Опубликовать**. Сохраненный плейбук будет готов к использованию и отобразится в таблице плейбуков со статусом **Активный**.

- Нажав на кнопку **Создать как черновик**. Это позволит вам создать плейбук, указав только его название и тенант, которому он принадлежит. Плейбук отобразится в списке плейбуков со статусом **Черновик**. Вы можете открыть его и продолжить вносить изменения.

  При сохранении плейбука в качестве черновика выполняется проверка, ошибки выделяются, но игнорируются.
  Вы можете сохранить плейбук только как черновик, если не построены связи между шагами выполнения и триггером, не настроены обязательные параметры или указаны недопустимые параметры.

Плейбук создан и отображается в списке плейбуков.

Настройка шагов выполнения плейбука в визуальном редакторе

После добавления шага выполнения плейбука при создании или изменении плейбука необходимо настроить его параметры. Для этого нажмите на блок с шагом, а затем в панели справа укажите необходимые параметры с помощью выражений jq.

В визуальном редакторе вы можете добавлять и настраивать следующие типы шагов выполнения плейбука:

- Реагирование
  - В списке **Тип действия** выберите тип действия по реагированию. Другие параметры зависят от выбранного типа.

    Типы действий по реагированию можно условно разделить **на группы**

    Действия по реагированию KATA/KEDR:

    - **Добавить правило запрета**

      Укажите активы, к которым следует применить действие, а также хеши SHA256 или MD5 файлов, которые вы хотите заблокировать.

    - **Удалить правило запрета**

      Укажите активы, к которым было применено правило запрета, и хеши файлов, которые нужно удалить.

    - **Сбросить правила запрета**

      Укажите активы, на которых необходимо сбросить правила запрета.

    - **Запуск приложения**

      Укажите параметры активов и исполняемого файла: полный путь к файлу в поле **Полный путь** и параметры, с которыми вы хотите запустить файл, в поле **Параметры командной строки**. В файле **Рабочая директория** вы можете указать путь к директории, в которой вы хотите сохранить результаты выполнения команды или файла.

    - **Включить сетевую изоляцию**

      Укажите активы, для которых вы хотите включить изоляцию, и период изоляции. Если вы хотите добавить исключение из правила сетевой изоляции, нажмите на кнопку **Добавить исключение** и укажите нужные параметры.

    - **Выключить сетевую изоляцию**

      Укажите активы, к которым была применена сетевая изоляция.

    Действия по реагированию через Active Directory:

    - **Заблокировать учетную запись**

      Укажите пользователей, учетные записи которых вы хотите заблокировать.

    - **Сбросить пароль**

      Укажите пользователей, для которых нужно сбросить пароль.

    - **Добавить пользователя в группу безопасности**

      Укажите пользователей и группу, в которую вы хотите добавить пользователей.

    - **Удалить пользователя из группы безопасности**

      Укажите пользователей и группу, из которой вы хотите удалить пользователей.

    Действие по реагированию Kaspersky Endpoint Security для Windows:

    - **Запустить поиск вредоносного ПО**

Укажите активы и тип проверки:

- **Проверка критических областей**.
- **Выборочная проверка**. Далее укажите путь к файлу, который вы хотите проверить.
- **Полная проверка**. При необходимости добавьте в проверку сетевые устройства, включив переключатель **Проверить сетевые диски**.

Если вы хотите, чтобы следующее действие по реагированию было запущено только после поиска вредоносного ПО, включите переключатель **Подождите завершения действия по реагированию**.

- **Обновить базы**

  Укажите устройства, на которых вы хотите обновить базы данных. Если вы хотите, чтобы следующее действие по реагированию было запущено только после обновления баз данных, включите переключатель **Подождите завершения действия по реагированию**.

- **Прервать процесс**

  Укажите устройства, на которых вы хотите прервать процесс. Выберите один из параметров и укажите выражение jq с необходимой информацией: **Хеш и путь** к файлу процесса, **Полный путь** к файлу или **PID** (идентификатор процесса).

  > В тех случаях, когда Kaspersky Endpoint Security со встроенным агентом работает в режиме EDR Expert, завершение процессов по системному PID не поддерживается.

- **Поместить на карантин**

  Укажите устройства, на которых находится файл, который нужно переместить. Затем выберите один из параметров и укажите выражение jq с необходимой информацией: **Полный путь** – путь к файлу, который вы хотите поместить на карантин, или **Хеш и путь** – хеш файла и путь к файлу.

Действие по реагированию Kaspersky Security Center:

- **Переместить в группу**

  Укажите устройства и путь к группе, в которую вы хотите переместить устройства.

Действие по реагированию Kaspersky Threat Intelligence Portal:

- **Обогатить данные**

  Выберите количество объектов для обогащения: все объекты или топ 100 объектов из источника. Укажите выражение jq с массивом наблюдаемых объектов для обогащения. Вы можете обогатить следующие типы наблюдаемых данных: MD5, SHA256, URL, домен или IP-адрес.

Изменение алертов или инцидентов с помощью плейбука:

- **Назначить пользователю или группе**

  Выберите пользователей или группы пользователей, которым вы хотите назначить алерт или инцидент.

- **Изменить атрибут внешней ссылки**

  Укажите выражение jq с атрибутом внешней ссылки алерта или инцидента, а затем выберите, следует ли перезаписать текущие выходные данные или объединить текущие и новые данные.

- **Изменить дополнительные данные**

  Выберите, следует ли перезаписать текущие выходные данные или объединить текущие и новые данные.

- **Изменить статус**

  Выберите статус алерта или инцидента: **Новый**, **В обработке** или **Закрыт**. Если областью действия плейбука являются инциденты, вам также нужно выбрать тип инцидента.

- **Изменить тип**

  Выберите тип инцидента.

  Этот тип реагирования доступен, если вы в раскрывающемся списке **Область действия** выбрали **Инцидент** при создании или изменении плейбука.

- **Изменить описание**

  Укажите выражение jq с описанием инцидента и выберите, следует ли перезаписать текущие выходные данные или объединить новые и текущие данные.

  Этот тип реагирования доступен, если вы в раскрывающемся списке **Область действия** выбрали **Инцидент** при создании или изменении плейбука.

- **Изменить приоритет**

  Выберите приоритет инцидента: **Критический**, **Высокий**, **Средний** или **Низкий**.

  Этот тип реагирования доступен, если вы в раскрывающемся списке **Область действия** выбрали **Инцидент** при создании или изменении плейбука.

- **Добавить комментарий**

  Укажите выражение jq с комментарием к алерту или инциденту.

- При необходимости в разделе **Дополнительные параметры** нажмите на значок стрелки (>) и **укажите дополнительные параметры**

  - Нажмите на кнопку **Прервать** или **Продолжить**, чтобы выбрать, следует ли прекратить или продолжить выполнение плейбука в случае возникновения ошибки.

  - Настройте время ожидания действия по реагированию. Вы можете выбрать параметр **Политика** и указать нужную политику времени ожидания; вы также можете выбрать параметр **Пользовательский** и указать время ожидания в часах.

  - Измените выходные данные плейбука, включив переключатель **Выходные данные**. В поле **Выход** укажите выражения jq для замены данных, возвращаемых действием по реагированию, а затем выберите метод замены **Объединить** или **Перезаписать**.

  - Вручную подтвердите вызов функции реагирования, включив переключатель **Ручное подтверждение**, а затем укажите время ожидания подтверждения в минутах. По умолчанию время ожидания составляет 60 минут.

    Если вы хотите включить уведомление по электронной почте, установите флажок **Отправить сообщение по электронной почте** и укажите задержку перед отправкой уведомления по электронной почте. Минимальное значение – 5 минут, максимальное – 30 минут. Также убедитесь, что соединение с SMTP-сервером настроено и адрес электронной почты указан в свойствах пользователя.

- **Цикл**

После выбора этого типа шага в визуальный редактор добавляются блоки **Цикл** и **Конец**.

- Нажмите на блок **Цикл** и укажите выражение jq для формирования массива входных данных, а затем выберите режим обработки элементов **Параллельно** или **Последовательно**.
- При необходимости в разделе **Дополнительные параметры** нажмите на значок стрелки (>) и **укажите дополнительные параметры**
  - Нажмите на кнопку **Прервать** или **Продолжить**, чтобы выбрать, следует ли прекратить или продолжить выполнение плейбука в случае возникновения ошибки.
  - В поле **Максимальный размер пакета** укажите количество элементов, которые плейбук может принимать в качестве входных данных.
  - Установите правила агрегации результатов выполнения плейбука по элементам входного массива. После включения переключателя **Агрегировать результаты** в поле **Выражение** укажите выражение jq, чтобы использовать выходные данные в качестве входных данных для следующих шагов выполнения.
  - Измените выходные данные, указав выражение jq в поле **Выход**.
  - Нажмите на кнопку **Объединить** или **Перезаписать**, чтобы выбрать, следует ли перезаписать текущие выходные данные или объединить новые и текущие данные.

- Параллельно

  После выбора этого типа шага в визуальный редактор добавляются блоки **Параллельно** и **Конец**.

  - Нажмите на блок **Параллельно** и укажите выражение jq для формирования массива входных данных, а затем введите названия веток.

    Вы можете добавить новые ветки, нажав на кнопку **Добавить ветку**.
  - При необходимости в разделе **Дополнительные параметры** нажмите на значок стрелки (>) и **укажите дополнительные параметры**
    - Нажмите на кнопку **Прервать** или **Продолжить**, чтобы выбрать, следует ли прекратить или продолжить выполнение плейбука в случае возникновения ошибки.
    - Установите правила агрегации результатов выполнения плейбука по элементам входного массива. После включения переключателя **Агрегировать результаты** в поле **Выражение** укажите выражение jq, чтобы использовать выходные данные для следующих шагов выполнения.
    - Измените выходные данные, указав выражение jq в поле **Выход**.
    - Нажмите на кнопку **Объединить** или **Перезаписать**, чтобы выбрать, следует ли перезаписать текущие выходные данные или объединить новые и текущие данные.

- Решение

  После выбора этого типа шага в визуальный редактор добавляются блоки **Решение** и **Конец**. Нажмите на блок **Решение** и укажите выражение jq с условием и имя условия.

  При необходимости добавьте новые условия, нажав на кнопку **Добавить условие**.

- Обновить данные

  Укажите выражения jq в поле **Выход** и выберите, следует ли перезаписать текущие входные данные или объединить новые и текущие данные.

С помощью шагов выполнения плейбука можно выполнить следующие действия:

- Изменять параметры, нажав на блок шага выполнения, а затем в открывшемся окне свойств изменить нужные параметры.

  Для параметров, подразумевающих ввод выражений jq, подсвечивается синтаксис и отображаются подсказки при начале ввода.

- Перемещаться по рабочей области визуального редактора, выбирая и перетаскивая блоки шагов выполнения.
- Удалять шаги выполнения, нажав на блок шага, а затем нажав клавишу **`Backspace`** или **`Delete`**.

В панели инструментов вы можете выполнить следующие действия:

- Открыть панель **Параметры плейбука**, нажав на кнопку **Параметры**.
- Открыть редактор кода с DSL-схемой, нажав на кнопку **Показать код**.

  Вы можете развернуть панель кода, нажав на значок (⌃), и закрыть панель, нажав на значок (×).

- Скопировать алгоритм из другого плейбука, нажав на кнопку **Копировать алгоритм**.
- Открыть историю реагирования на плейбуки, нажав на кнопку **Просмотреть историю реагирований**.
- Эмулировать запуск плейбука без фактического выполнения реагирования с помощью кнопки **Запустить в тестовом режиме**.
- Отменить любое действие в визуальном редакторе, нажав на кнопку **Отменить**.
- Вернуть ранее отмененное действие, нажав на кнопку **Повторить**.
- Автоматически выровнять элементы, нажав на кнопку **Упорядочить**.

Изменение плейбуков

Чтобы изменить плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Для предустановленных плейбуков вы можете изменить только режим плейбука и правило запуска. Вы также можете просматривать алерты или инциденты, соответствующие предустановленному сценарию.

Вы можете изменить плейбук, только если у вас есть разрешение на изменение тенанта, которому принадлежит плейбук.

Чтобы изменить плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.

2. Выберите плейбук, который требуется изменить.

3. В открывшемся окне измените свойства плейбука. Дополнительные сведения о свойствах плейбука, которые вы можете изменить, см. в разделе Создание плейбуков.

4. Если вы изменили режим работы на **Автоматический**, в раскрывающемся списке **При одновременном запуске нескольких экземпляров плейбука** выберите одно из следующих действий:

   - **Добавить экземпляры плейбука в очередь**. Новый экземпляр плейбука будет запущен после завершения текущего. По умолчанию выбрано это действие.

   - **Завершить текущее выполнение и запустить новый экземпляр**. Выполнение текущего экземпляра плейбука будет прекращено. После этого запускается новый экземпляр плейбука.

   - **Не запускать новые экземпляры плейбука**. Новый экземпляр плейбука не будет запущен. Выполнение текущего экземпляра плейбука будет продолжено.

5. Если вы измените режим работы на режим **Ручной**, в раскрывающемся списке **Действие с запущенными экземплярами плейбука** выберите действие, которое будет применяться к запуску экземпляров плейбуков:

   - **Завершение экземпляров, которые выполняются или ожидают утверждения**.

   - **Завершение тех экземпляров, которые ожидают подтверждения**.

   - **Выполнить все экземпляры, которые выполняются или ожидают утверждения**.

6. Сохраните изменения, нажав на кнопку **Сохранить**.

   Вы также можете нажать на кнопку **Сохранить с комментарием**, если хотите добавить комментарий к плейбуку перед сохранением.

Свойства плейбука изменены и сохранены.

Настройка плейбуков

Вы можете настроить любой плейбук как вам нужно.

Чтобы настроить плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.

2. Откройте плейбук для изменения, выбрав его из списка и нажав на кнопку **Дублировать и изменить**.

3. В открывшемся окне измените свойства плейбука в соответствии с вашими требованиями.

   Дополнительные сведения о свойствах плейбука, которые вы можете изменить, см. в разделе Создание плейбуков.

   Если вы хотите настроить параметры алгоритма плейбука, см. раздел Алгоритм плейбука.

Имя настраиваемого плейбука должно быть уникальным.

4. Нажмите на кнопку **Сохранить**.

   Настраиваемый плейбук будет изменен и сохранен.

Просмотр свойств плейбука

Плейбуки позволяют автоматизировать рабочие процессы и сокращать время, необходимое для обработки алертов и инцидентов.

Чтобы просматривать плейбуки, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор, Администратор тенанта.

Чтобы просмотреть свойства плейбука:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.

2. В списке плейбуков нажмите на название плейбука, который вы хотите просмотреть.

   Открывшееся окно содержит информацию о плейбуке.

Справа в панели **Параметры плейбука** отображается следующая общая информация:

- **Тенант и наследование**. Имя тенанта, которому принадлежит плейбук.
- **Название**. Название плейбука.
- **Область действия**. Область действия плейбука. Возможные значения: **Алерт** или **Инцидент**.
- **Режим работы**. Режим работы плейбука. Возможные значения: **Автоматический**, **Обучение**, **Ручной**.

  Если режим выбран режим работы плейбука **Автоматический**, отображается поле **При одновременном запуске нескольких экземпляров плейбука**. Возможные значения: **Не запускать новые экземпляры плейбука**, **Завершить текущее выполнение и запустить новый экземпляр**, **Добавить экземпляры плейбука в очередь**.
- **Теги**. Теги, присвоенные плейбуку.
- **Описание**. Описание плейбука.
- **Дополнительные параметры**. Необязательные параметры, указанные при создании плейбука.

В рабочей области визуального редактора слева отображаются триггер и алгоритм плейбука (шаги выполнения плейбука).

Вы можете изменить свойства плейбука, если у вас есть одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Вы можете просмотреть историю действий по реагированию на плейбук, нажав на кнопку **Просмотреть историю реагирований** в панели инструментов. Откроется список всех плейбуков или действий по реагированию, запущенных в рамках плейбука. Вы можете прервать запущенные плейбуки или действия по реагированию, нажав на кнопку **Прервать**.

Если необходимо вы можете группировать и фильтровать данные в таблице следующим образом:

- Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

  Если вы применяете фильтр для столбца **Статус**, таблица отображает вручную запущенные действия по реагированию, статус которых содержит выбранное значение, и плейбуки, которые включают действия по реагированию, статус которых содержит выбранное значение. В этом случае будут отображаться только те действия по реагированию плейбука, которые соответствуют критерию фильтра.

Отобразится отфильтрованная таблица плейбуков.

Таблица содержит следующие столбцы:

- **Действия**. Название действия по реагированию.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в алгоритме плейбука.
- **Начало**. Дата и время запуска плейбука или действия по реагированию.
- **Конец**. Дата и время завершения плейбука или действия по реагированию.
- **ID алерта или инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.
- **Запущено**. Имя пользователя, запустившего плейбук или действие по реагированию.
- **Подтверждающий**. Имя пользователя, подтвердившего запуск плейбука или действия по реагированию.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров (⚙) и выберите столбец **Подтверждающий**.
- **Время подтверждения**. Дата и время, когда пользователь подтвердил или отклонил запуск плейбука или действие по реагированию.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров (⚙) и выберите столбец **Время подтверждения**.
- **Статус**. Статус выполнения плейбука. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – плейбук ожидает подтверждения для запуска.
  - **В обработке** – плейбук выполняется.
  - **Успешно** – плейбук завершен без ошибок или предупреждений.
  - **Предупреждение** – плейбук завершен с предупреждениями.
  - **Ошибка** – плейбук завершен с ошибками.

- **Прервано** – плейбук завершен, так как пользователь прервал выполнение.
- **Истекло время подтверждения** – плейбук завершен, так как время для подтверждения запуска истекло.
- **Отклонено** – плейбук завершен, так как пользователь отклонил запуск.

Вы можете нажать на значение **Статус**, чтобы открыть окно с результатом запуска плейбуков. Идентификатор запуска может использоваться Службой технической поддержки для загрузки данных, необходимых для анализа в случае ошибок выполнения. По умолчанию данные хранятся 72 часа.
Если статус плейбука равен **В обработке**, вы можете просмотреть идентификатор запуска, наведя курсор мыши на значок рядом со статусом.

- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе. Поле пустое, если плейбук или действие по реагированию не включают активы.

Вы также можете просмотреть историю действий по реагированию в разделе **История реагирований** или в деталях алерта или инцидента.

Прерывание работы плейбуков

Вы можете принудительно прервать запущенный плейбук. В этом случае незавершенные действия по реагированию будут прерваны. Завершенные действия по реагированию не будут отменены после завершения плейбука.

Чтобы прервать плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы прервать плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. В списке плейбуков выполните одно из следующих действий:
   - Выберите нужный плейбук, а затем в панели инструментов нажмите на кнопку **Просмотреть историю**.
   - Нажмите на название нужного плейбука, а затем в открывшемся окне нажмите на кнопку **Просмотреть историю**.
3. Выберите **Просмотреть историю реагирований**.

   Откроется панель со списком запущенных экземпляров плейбуков.
4. Выберите один или несколько экземпляров плейбуков, которые вы хотите завершить, затем нажмите на кнопку **Прервать** и подтвердите свой выбор.

Плейбук прерван.

Удаление плейбуков

Предустановленные плейбуки невозможно удалить.

Чтобы удалить пользовательский плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы удалить пользовательский плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. Выберите плейбук из списка и нажмите на кнопку **Удалить**.
3. В диалоговом окне нажмите на кнопку **Удалить**.

   Плейбук невозможно удалить, если есть запущенные экземпляры плейбука. В этом случае завершите все запущенные экземпляры перед удалением плейбука.

Если вы удалили плейбук со статусом **Активный** или **Недоступно**, он отобразится в таблице плейбуков со статусом **Удалено** и будет доступен только для просмотра и копирования.

Плейбуки со статусом **Удалено** удаляются навсегда.

Управление версиями плейбука

Kaspersky EDR Expert хранит историю версий плейбуков. Новая версия создается автоматически, когда вы создаете плейбук или сохраняете изменения в существующем плейбуке. Вы можете управлять версиями плейбука только после их публикации. Управление версиями не применяется к черновикам плейбука.

Недавно опубликованному плейбуку назначается версия `1`. Каждый раз, когда вы сохраняете изменения, номер версии увеличивается на единицу. Последняя сохраненная версия в списке версий помечается как `Текущая`.

Если вы обновляете Kaspersky EDR Expert с версии 2.0, версия плейбука будет назначена существующему плейбуку после того, как вы измените его в первый раз. Предыдущая версия существующего плейбука также будет сохранена и доступна для сравнения с последней версией.

Сравнение версий плейбука

Kaspersky EDR Expert позволяет сравнивать разные версии плейбука, чтобы отслеживать изменения и восстанавливать предыдущие версии.

Для этого вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Чтобы сравнить версии плейбука:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. В списке плейбуков выберите плейбук, версии которого вы хотите сравнить.
3. Нажмите на кнопку **Просмотреть историю** и выберите **Просмотреть историю версий**.

   Откроется окно **История версий плейбука**.
4. В списке версий плейбука выберите две версии для сравнения и нажмите на кнопку **Сравнить**.

   Откроется окно, в котором отображаются различия между версиями плейбука. Обратите внимание, что вы не можете изменить плейбук в этом окне.

   При необходимости в открывшемся окне вы можете выбрать разные версии плейбука для сравнения.

Сравнение версий плейбука выполнено.

Восстановление версий плейбука

Вы можете восстановить предыдущую версию плейбука в любое время.

Для этого вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик SOC, Аналитик 1-го уровня, Аналитик 2-го уровня.

Чтобы восстановить версию плейбука:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. В списке плейбуков выберите плейбук, версию которого вы хотите восстановить.

   Также вы можете нажать на название плейбука.
3. Нажмите на кнопку **Просмотреть историю** и выберите **Просмотреть историю версий**.

   Откроется окно **История версий плейбука**.
4. В списке версий плейбука найдите версию, которую вы хотите восстановить.

   Если вы хотите просмотреть сведения о выбранной версии плейбука, нажмите на номер версии.
5. В столбце **Действие** нажмите на кнопку **Восстановить**.

6. В открывшемся окне подтверждения нажмите **Восстановить**.

   При необходимости, добавьте комментарий. Если вы не добавите комментарий, он будет добавлен автоматически с указанием версии, из которой был восстановлен плейбук.

Предыдущая версия плейбука восстановлена.

Запуск плейбука в тестовом режиме

Вы можете запускать плейбуки в тестовом режиме, чтобы выполнить отладку или проверить результат. Во время тестового запуска плейбук обрабатывает выбранные алерты и инциденты, но не выполняет никаких действий с активами.

Запуск в тестовом режиме доступен для плейбуков с любым статусом.

Чтобы запустить плейбук в тестовом режиме, вам должна быть присвоена одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы запустить плейбук в тестовом режиме:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.

2. Выполните одно из следующих действий:

   - Выберите плейбук, который требуется изменить. В открывшемся окне **Сведения о плейбуке** нажмите на кнопку **Запустить в тестовом режиме**.

   - Выберите плейбук из списка и нажмите на кнопку **Запустить в тестовом режиме**.

     В зависимости от области действия плейбука откроется панель **Выбрать инцидент** или **Выбрать алерт**.

3. В открывшейся панели выберите инцидент или алерт.

   Если для плейбука требуется выбрать наблюдаемые объекты и активы, включите параметр **Выберите целевые объекты перед запуском плейбуков**.

4. Нажмите **Запустить**.

   Если вы включили параметр **Выберите целевые объекты перед запуском плейбуков**, откроется панель **Целевые объекты**. Выберите объекты на вкладках **Наблюдаемые объекты** и **Активы**, для которых вы хотите запустить плейбук, и нажмите на кнопку **Применить и запустить**.

5. Отобразится всплывающее окно **Плейбук запущен в тестовом режиме**. После завершения тестового запуска отобразится всплывающее окно **Плейбук завершен в тестовом режиме**. Во всплывающем окне нажмите **Показать результат**, чтобы открыть панель с результатами. Если тестовый запуск пройдет успешно, отобразится панель **Плейбук** с сообщением об успешном выполнении. Если тестовый запуск завершится неудачно, отобразится панель **Плейбук** с сообщением об ошибке.

   Результаты тестового запуска сохраняются в разделе **История реагирований** свойств плейбука. Результаты тестового запуска не отображаются в общем разделе История реагирований.

Запуск плейбуков и действий по реагированию

Запуск плейбуков

В зависимости от ваших требований вы можете настроить способ запуска плейбука. При создании плейбука вы можете выбрать один из следующих режимов работы:

- **Автоматический**. Выберите этот режим работы, если вы хотите запускать автоматически плейбуки и действия по реагированию.

  Плейбуки в этом режиме помогают автоматизировать реагирование на угрозы, а также сокращают время, необходимое для анализа алертов и инцидентов.

- **Обучение**. Выберите этот режим работы, если вы хотите проверить, правильно ли настроен плейбук.

  Плейбуки в этом режиме не будут запускаться автоматически при обнаружении соответствующего алерта или инцидента. Вместо этого плейбук запрашивает подтверждения пользователя на запуск.

- **Ручной**. Выберите этот режим работы, если вы хотите запускать плейбук только вручную.

  У плейбуков в этом режиме нет триггера, поэтому вы можете запускать такие плейбуки для любого алерта или инцидента, в зависимости от выбранной области действия плейбука. Дополнительные сведения см. в разделе Запуск плейбуков вручную.

Также можно изменить режим работы плейбука. Дополнительные сведения см. в разделе Изменение плейбуков.

Запуск действий по реагированию

Действия по реагированию могут запускаться вручную, автоматически в рамках плейбука или могут быть настроены на запрос подтверждения пользователя перед запуском в плейбуке. По умолчанию ручное подтверждение действия по реагированию выключено.

Дополнительные сведения о настройке ручного подтверждения действия по реагированию, запущенного в плейбуке, см. в разделе Настройка ручного подтверждения плейбуков и ответных действий.

Запуск плейбуков вручную

Kaspersky EDR Expert позволяет вручную запускать любой плейбук, соответствующий алертам или инцидентам, на которые требуется реагировать.

> Чтобы запустить плейбук вручную, вам должна быть присвоена одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Вы также можете запустить плейбук для наблюдаемых объектов и активов, если вы указали эти объекты при создании плейбука и при его запуске.

Запуск плейбука для алерта

Чтобы запустить плейбук вручную для алерта:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**.
2. В таблице алертов нажмите на ссылку с идентификатором, для которого вы хотите запустить плейбук.
3. В открывшемся окне **Детали алерта** нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.
4. В списке плейбуков, соответствующих алертов, выберите плейбук, который вы хотите запустить и нажмите на кнопку **Запустить**.

   Если выбранный плейбук уже запущен для этого алерта, в открывшемся окне **Мониторинг**, выполните одно из следующих действий:

   - Если вы хотите дождаться завершения текущего экземпляра плейбука, нажмите на кнопку **Подождите и запустите**.

     Новый экземпляр плейбука будет запущен после завершения текущего.
   - Если вы хотите немедленно запустить новый экземпляр плейбука, нажмите на кнопку **Прервать и запустить новый**.

     Текущий экземпляр плейбука будет прерван, а новый будет запущен.
   - Если вы хотите отменить запуск нового плейбука, нажмите на кнопку **Закрыть** (×).

   > Если выбранный плейбук уже имеет статус **Ожидание подтверждения**, после запуска вручную его статус изменится на **Запущено**.

Плейбук запускается для выбранного алерта. После того как плейбук будет завершен, вы получите уведомление.

Запуск плейбука для инцидента

Чтобы запустить плейбук вручную для инцидента:

1. В главном меню перейдите в раздел **Мониторинг** → **Инциденты** и выберите вкладку **XDR-инциденты**.
2. В таблице инцидентов перейдите по ссылке с идентификатором, для которого вы хотите запустить плейбук.
3. В открывшемся окне **Детали инцидента** нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.
4. В списке плейбуков, соответствующие инциденту, выберите плейбук, который вы хотите запустить и нажмите на кнопку **Запустить**.

Если выбранный плейбук уже запущен для этого инцидента, в открывшемся окне **Мониторинг**, выполните одно из следующих действий:

- Если вы хотите дождаться завершения текущего экземпляра плейбука, нажмите на кнопку **Подождите и запустите**.

  Новый экземпляр плейбука будет запущен после завершения текущего.

- Если вы хотите немедленно запустить новый экземпляр плейбука, нажмите на кнопку **Прервать и запустить новый**.

  Текущий экземпляр плейбука будет прерван, а новый будет запущен.

- Если вы хотите отменить запуск нового плейбука, нажмите на кнопку **Закрыть** (×).

> Если выбранный плейбук уже имеет статус **Ожидание подтверждения**, после запуска вручную его статус изменится на **Запущено**.

Плейбук будет запущен для выбранного инцидента. После того как плейбук будет завершен, вы получите уведомление.

Запуск плейбуков для объектов, указанных пользователями

Вы можете указать наблюдаемые объекты и активы, для которых должен выполняться плейбук. Для этого вам нужно создать плейбук со следующими параметрами:

- В списке **Область действия** выбрать **Алерт** или **Инцидент**.
- В списке **Режим работы** выбрать **Ручной**.
- В рабочей области визуального редактора при Настройка шагов выполнения плейбука в визуальном редакторе, используйте выражения jq, чтобы указать объекты (наблюдаемые объекты или активы), для которых вы хотите запустить плейбук. Эти объекты будут входными данными для плейбука при его запуске.

> Если вы не укажете объекты в алгоритме плейбука и выберете их только перед запуском плейбука, эти объекты будут проигнорированы.

После того как плейбук создан, вы можете запустить его для выбранных объектов.

> Для этого вам должна быть присвоена одна из следующих EDR-ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

Чтобы запустить плейбук для выбранных объектов:

1. В главном меню перейдите в раздел **Мониторинг**, а затем в разделе **Алерты** или **Инциденты** нажмите на идентификатор алерта или инцидента, из которого вы хотите запустить плейбук.
2. В открывшемся окне нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.

3. Выберите параметр **Установите флажок Выберите целевые объекты перед запуском плейбуков** и нажмите на кнопку **Запустить**.

4. В открывшемся окне **Целевые объекты** выберите объекты на вкладках **Наблюдаемые объекты** и **Активы**, для которых вы хотите запустить плейбук, и нажмите на кнопку **Применить и запустить**.

   Плейбук будет запущен для выбранного объекта.

Вы можете просмотреть результат плейбука на вкладке **История** в сведениях алерта или инцидента, из сведений плейбука или таблицы плейбуков нажав на кнопку **Просмотреть историю**, и в разделе История реагирования.

Например, вы пишете скрипт, который вызывается во время действия по реагированию executeCustomScript. При создании плейбука в рабочей области визуального редактора добавляется шаг выполнения **Запустить пользовательский скрипт** с входными данными плейбука. Затем вам нужно запустить скрипт для наблюдаемого объекта с типом IP, который вы выбираете при запуске плейбука. Скрипт использует IP-адрес, который вы выбрали в качестве параметра:

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "executeCustomScript",
                    "params": {
                        "commandLine": "./script.py",
                        "commandLineParameters": "${ \"-ip \" + ([.input.observables[] | select(.type == \"ip\")]
| map(.value) | join(\",\")) }",
                        "workingDirectory": "/folder/with/script"
                    }
                },
                "onError": "stop"
            }
        },
      {
        "action": {
          "function": {
            "type": "updateBases",
            "params": {
              "wait": false
            },
            "assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
          }
        }
      }
    ]
}
```

Несколько объектов будут входными данными для плейбука, а список IP-адресов, разделенных запятыми, должны быть входными данными для скрипта:

```
{
    "input": {
        "observables": [
            {
                "type": "ip",
                "value": "127.0.0.1"
            },
            {
                "type": "ip",
                "value": "127.0.0.2"
            },
            {
                "type": "md5",
                "value": "29f975b01f762f1a6d2fe1b33b8e3e6e"
            }
        ],
```

```
        "assets":[
      {
         "AttackerOrVictim": "unknown",
         "ID": "c13a6983-0c40-4986-ab30-e85e49f98114",
         "InternalID": "6d831b04-00c2-44f4-b9e3-f7a720643fb7",
         "KSCServer": "E5DE6B73D962B18E849DC0BF5A2BA72D",
         "Name": "VIM-W10-64-01",
         "Type": "host"
      }
   ]
}
```


После того как выражения jq выполнят вычисления с операционными данными плейбука, следующая информация передается в качестве параметров командной строки:

```
-ip 127.0.0.1,127.0.0.2
```

Для плейбука, ожидающего входных данных, если вы указали разные типы объектов при создании плейбука и при его запуске или если вы не выбрали параметр **Выбрать целевые объекты перед запуском плейбука**, плейбук завершится с одним из следующих результатов:

- Произойдет ошибка, поскольку плейбук не получил входных данных.
- Действие не будет выполнено, поскольку плейбук содержит условие или цикл, основанный на входных данных.
- Результат будет зависеть от ответа приложения, службы или скрипта, выполняющего действие.

Запуск плейбуков в режиме Обучение

Режим работы **Обучение** позволяет вам проверять, правильно ли настроен плейбук. Это может быть полезно, если вы планируете изменить режим работы плейбука на **Автоматический**.

Все плейбуки в режиме **Обучение** требуют подтверждения запуска пользователем.

> Чтобы запустить плейбук в режиме работы **Обучение**, вам должна быть присвоена одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

В режиме работы **Обучение** плейбук запускается алертами или инцидентами, но требует ручного подтверждения перед запуском. Вы можете протестировать запуск плейбука в режиме работы **Обучение** одним из следующих способов:

- Создайте алерт или инцидент, соответствующий триггеру плейбука.
- Измените алерт или инцидент, соответствующий триггеру плейбука. Алерт или инцидент должны иметь статус, отличный от **Закрыт**.

  > Изменение алерта или инцидента запускает плейбук, только если триггер настроен на реагирование на изменения вручную. По умолчанию изменения, вручную внесенные в алерт или инцидент, игнорируются. Чтобы плейбук реагировал на изменения вручную, триггер должен использовать функцию `event.manual`. Подробную информацию см. в разделе Триггеры плейбука.

Когда одно из вышеуказанных действий выполнено, плейбук запрашивает подтверждение пользователя для запуска. Дополнительные сведения о том, как подтвердить плейбук, см. в разделе Подтверждение плейбуков или действий по реагированию.

Подтвердить запуск плейбука вручную можно в течение 60 минут.

Настройка ручного подтверждения действий по реагированию

Kaspersky EDR Expert позволяет настроить подтверждение действия по реагированию, запущенное в пользовательском плейбуке, вручную. По умолчанию ручное подтверждение действия по реагированию выключено.

Перед настройкой подтверждения вручную убедитесь, что настроены уведомления по электронной почте для тенантов и указан адрес электронной почты подтверждающего.

Рекомендуется настроить ручное подтверждение следующих действий по реагированию: перемещение устройств в другую группу администрирования, перемещение файлов на карантин, включение и выключение сетевой изоляции, реагирование на учетные записи с помощью Active Directory и обогащение данных.

Чтобы настроить подтверждение действия по реагированию вручную:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Плейбуки**.
2. Откройте плейбук для изменения, выполнив одно из следующих действий:
   - Выберите плейбук, который требуется изменить. В открывшемся окне **Сведения о плейбуке** нажмите на кнопку **Изменить**.
   - Выберите плейбук из списка и нажмите на кнопку **Изменить**.

     Если вы выберете более одного плейбука, кнопка **Изменить** будет неактивна.

   Откроется окно **Настроить плейбук**.
3. В разделе **Алгоритм** укажите один из следующих параметров действия по реагированию, для которого вы хотите включить подтверждение вручную:
   - Чтобы включить подтверждение действия по реагированию вручную со временем подтверждения по умолчанию, укажите следующий параметр:

     ```
     "manualApprove": true
     ```

     По умолчанию время подтверждения составляет 60 минут.

- Чтобы разрешить подтверждение действия по реагированию вручную с настраиваемым временем подтверждения, укажите следующий параметр:

```
"manualApprove": {"timeout": "period"}
```

  где `"период"` – регулируемое время подтверждения.

  Вы можете настроить время подтверждения в часах (h) и/или минутах (m), например:

```
"manualApprove": {"timeout": "20h"}
"manualApprove": {"timeout": "2h30m"}
```

- Чтобы включить ручное подтверждение действия по реагированию с уведомлениями, отправляемыми на адрес электронной почты подтверждающего, укажите следующий параметр:

```
"emailNotifications": {
 "enabled":true
}
```

- Чтобы включить ручное подтверждение действия по реагированию с уведомлением, которое отправляется на адрес электронной почты подтверждающего по прошествии определенного периода времени, укажите следующий параметр:

```
"manualApprove": {
  "emailNotifications": {
    "enabled": true,
    "delay": "period"
  }
```

  где `"период"` – регулируемое время отправления.

  Вы можете настроить время отправки в минутах, например:

```
"delay": "20m"
```

4. Нажмите на кнопку **Сохранить**.

   Подтверждение действия по реагированию вручную настроено. Уведомления по электронной почте с запросом на подтверждение действия по реагированию будут отправлены на адрес электронной почты, указанный в свойствах учетной записи пользователя.

Вы можете просмотреть запросы на подтверждение действия по реагированию в разделе **Запросы о подтверждении**.

Подтверждение плейбуков или действий по реагированию

Все плейбуки в режиме **Обучение** требуют подтверждения пользователя. Вы также можете настроить подтверждение вручную действий по реагированию, запускаемых в плейбуках.

Для подтверждения или отклонения плейбука необходима одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы утвердить или отклонить запуск действия по реагированию, вам должна быть присвоена из следующих ролей: Главный администратор, Подтверждающий, Администратор тенанта.

Если есть плейбуки или действия по реагированию, ожидающие подтверждения пользователя, в верхней части Консоли OSMP отображается уведомление. Также если для запуска действия по реагированию требуется подтверждение пользователя, на адрес электронной почты отправляется уведомление в течение периода, указанного в алгоритме плейбука.

Просмотр списка плейбуков и действий по реагированию

Чтобы просмотреть список плейбуков и действий по реагированию, ожидающих подтверждения, выполните одно из следующих действий:

- Перейдите по ссылке **Просмотр запросов о подтверждении** в верхней части Консоли OSMP.
- Перейдите по ссылке в уведомлении, которое было отправлено на ваш адрес электронной почты.

Откроется панель **Запросы о подтверждении**, содержащая полный список запросов на подтверждение.

Таблица **Запросы о подтверждении** содержит следующие столбцы:

- **Время**. Дата и время, когда плейбук или действие по реагированию запросили подтверждения пользователя.
- **Срок утверждения**. Дата и время, до которых пользователь должен подтвердить или отклонить плейбук или действие по реагированию. Если к этому времени пользователь не подтвердил плейбук или действие по реагированию, запуск отменяется.
- **Плейбук**. Имя пользовательского или предустановленного плейбука, который запрашивает подтверждение пользователя.
- **Действие по реагированию**. Действия, запускаемые в плейбуках.
- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете просмотреть список активов, для которых требуется подтверждение пользователя, нажав на ссылку с количеством активов.

- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию или алгоритме плейбука.
- **ID алерта или инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.

Подтверждение и отклонение плейбуков

Чтобы подтвердить или отклонить плейбук:

1. В уведомлении в верхней части Консоли OSMP нажмите на ссылку **Просмотр запросов о подтверждении**.

   > Уведомление со ссылкой **Просмотр запросов о подтверждении** отображается только в том случае, если существует плейбук, ожидающий подтверждения пользователя.

2. В открывшейся панели **Запросы о подтверждении** выберите один или несколько плейбуков, а затем выполните одно из следующих действий:

   - Чтобы подтвердить запуск плейбука, нажмите на кнопку **Одобрить**.

     После этого плейбук запускается. Статус действия **История реагирований** изменится на **В обработке**.

   - Чтобы отклонить запуск плейбука, нажмите на кнопку **Отклонить**.

     После этого запуск плейбука отменен. Статус действия **История реагирований** изменится на **Отклонено**.

3. Нажмите на кнопку **Закрыть** (×), чтобы закрыть панель **Запросы о подтверждении**.

После подтверждения или отклонения плейбуков вы можете просмотреть их статусы в разделе **История реагирований**.

Подтверждение и отклонение действий по реагированию

Чтобы подтвердить или отклонить действия по реагированию:

1. В уведомлении в верхней части Консоли OSMP нажмите на ссылку **Просмотр запросов о подтверждении**.

   > Уведомление со ссылкой **Просмотр запросов о подтверждении** отображается только в том случае, если существует действие по реагированию, ожидающее подтверждения пользователя.

   Откроется панель **Запросы о подтверждении**.

2. В открывшейся панели **Запросы о подтверждении** в столбце **Активы** перейдите по ссылке с количеством активов.

   Откроется панель **Активы для подтверждения**, содержащая полный список активов.

3. Проверьте список активов, для которых требуется подтверждение вручную, а затем выполните одно из следующих действий:

   - Чтобы подтвердить запуск действия по реагированию для активов, выберите один или несколько активов, которые вам нужны, а затем нажмите на кнопку **Одобрить**. После этого запускается действие по реагированию для выбранных активов.

   - Чтобы отклонить запуск действия по реагированию для активов, выберите один или несколько активов, которые вам нужны, а затем нажмите на кнопку **Отклонить**. После этого запуск действия по реагированию для выбранных активов отменяется.

4. Нажмите на кнопку **Закрыть** (×), чтобы закрыть панель **Активы для подтверждения**.

5. Нажмите на кнопку **Закрыть** (×), чтобы закрыть панель **Запросы о подтверждении**.

После подтверждения или отклонения действий по реагированию вы можете просмотреть их статусы в разделе **История реагирований**.

Обогащение из плейбуков

После настройки интеграции между Kaspersky EDR Expert и Kaspersky TIP вы можете получить информацию о репутации наблюдаемых объектов, связанных с алертом или инцидентом, из Kaspersky TIP или Kaspersky OpenTIP, а затем дополнить полученные данные.

> Вы можете получить информацию только для наблюдаемых объектов следующего типа: домен, URL, IP, MD5, SHA256.

Вы можете настроить автоматическое обогащение данных. Для этого при создании или изменении плейбука в рабочей области визуального редактора нужно добавить раздел Настройка шагов выполнения плейбука в визуальном редакторе и указать следующее:

1. Ограничьте количество данных, возвращаемых Kaspersky TIP или Kaspersky OpenTIP, если это необходимо.

   Вы можете указать одно из следующих значений:

   - Все записи.

   - Top100

     > Это значение установлено по умолчанию.

2. Наблюдаемый объект, для которого плейбук запрашивает данные у Kaspersky TIP или Kaspersky OpenTIP.

   > Обогащение данных осуществляется с помощью сервиса, указанного в интеграции с Kaspersky Threat Intelligence Portal.

В алгоритме плейбука вы можете использовать параметры обогащения вывода, отображаемые в полях, которые возвращает Kaspersky TIP.

Вы можете просмотреть результат обогащения для всех наблюдаемых объектов, связанных с алертом или инцидентом, одним из следующих способов:

- в деталях алерта или инцидента;
- в истории реагирования;
- в плейбуке.

Чтобы просмотреть результат обогащения:

1. В главном окне приложения перейдите в раздел **Мониторинг** и выполните одно из следующих действий:
   - Если вы хотите просмотреть результат из деталей алерта или инцидента, перейдите в раздел **Алерты** или **Инциденты** и нажмите на идентификатор алерта или инцидента, для которого было выполнено обогащение. В открывшемся окне выберите вкладку **История** и перейдите на вкладку **История реагирования**.
   - Если вы хотите просмотреть результат в истории действий по реагированию, перейдите в раздел **История реагирований**.
   - Если вы хотите просмотреть результат из таблицы плейбука, перейдите в раздел **Плейбуки** и выполните одно из следующих действий:
     - Выберите плейбук, для которого было выполнено обогащение. В панели инструментов нажмите на кнопку **Просмотреть историю** и выберите **Просмотреть историю реагирований**.
     - Нажмите на название плейбука, для которого было выполнено обогащение. В открывшемся окне нажмите на кнопку **Просмотреть историю** и выберите **Просмотреть историю реагирований**.
2. В столбце **Статус действия** нажмите на статус плейбука, для которого вы хотите просмотреть результаты обогащения.

Вы также можете получить информацию из Kaspersky TIP и дополнить данные вручную на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента.

Просмотр истории реагирования

Раздел **История реагирований** позволяет просматривать подробную историю реагирования для всех обнаруженных алертов и инцидентов. Обратите внимание, что при удалении алерта или инцидента история реагирования для этого алерта или инцидента не отображается.

> Чтобы просмотреть историю действия по реагированию, у вас должна быть одна из следующих ролей: Главный администратор, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Младший аналитик, Подтверждающий, Аудитор, Администратор тенанта.

Чтобы просмотреть историю реагирования, в главном меню перейдите в раздел **Мониторинг** → **История реагирований**. Откроется таблица с историей реагирования на все алерты и инциденты.

По умолчанию таблица сортируется в соответствии с временем запуска плейбука или действия по реагированию. Действия по реагированию в плейбуках упорядочены в соответствии с их порядком в алгоритме плейбука.

Панель инструментов в верхней части таблицы позволяет группировать и фильтровать данные в таблице следующим образом:

- Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

> Если вы применяете фильтр для столбца **Статус действия**, таблица отображает вручную запущенные действия по реагированию, статус которых содержит выбранное значение, и плейбуки, которые включают действия по реагированию, статус которых содержит выбранное значение. В этом случае будут отображаться только те действия по реагированию плейбука, которые соответствуют критерию фильтра.

Поиск по таблице доступен по всем столбцам, кроме **Статус действия** и **Статус плейбука**. Чтобы отфильтровать данные в этих столбцах, нажмите на заголовок столбца и выберите нужный статус в раскрывающемся списке.

Таблица содержит следующие столбцы:

- **Действия**. Название действия по реагированию или плейбука.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию или алгоритме плейбука.
- **Начало**. Дата и время запуска плейбука или действия по реагированию.
- **Конец**. Дата и время завершения плейбука или действия по реагированию.
- **ID алерта или инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.
- **Запущено**. Имя пользователя, запустившего плейбук или действие по реагированию.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **В обработке** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.

Устройства, на которых была включена сетевая изоляция, могут получить статус **Успешно** раньше, чем процесс изоляции будет завершен.

- **Статус плейбука**. Статус выполнения плейбука. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – плейбук ожидает подтверждения для запуска.
  - **В обработке** – плейбук выполняется.
  - **Успешно** – плейбук завершен без ошибок или предупреждений.
  - **Предупреждение** – плейбук завершен с предупреждениями.
  - **Ошибка** – плейбук завершен с ошибками.
  - **Прервано** – плейбук завершен, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – плейбук завершен, так как время для подтверждения запуска истекло.
  - **Отклонено** – плейбук завершен, так как пользователь отклонил запуск.

  Вы можете нажать на значение **Статус плейбука** или на значение **Статус действия**, чтобы открыть окно с результатом запуска плейбука или действия по реагированию. Идентификатор запуска, отображающийся на вкладке **Отладка данных**, может использоваться Службой технической поддержки для скачивания данных, необходимых для анализа в случае ошибок выполнения. По умолчанию данные хранятся 72 часа.
  Если статус плейбука равен **В обработке**, вы можете просмотреть идентификатор запуска, наведя курсор мыши на значок рядом со статусом.

- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе. Поле пустое, если плейбук или действие по реагированию не включают активы.

- **Тенант**. Имя тенанта, которому принадлежит плейбук.

- **Подтверждающий**. Имя пользователя, который подтвердил или отклонил запуск плейбука или запуск действия по реагированию.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров (⚙) и выберите столбец **Подтверждающий**.

- **Время подтверждения**. Дата и время, когда плейбук или действие по реагированию были подтверждены или отклонены. По умолчанию этот столбец не отображается.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров (⚙) и выберите столбец **Время подтверждения**.

Предустановленные плейбуки

Kaspersky EDR Expert предоставляет готовые предустановленные плейбуки, созданные экспертами "Лаборатории Касперского". Предустановленные плейбуки основаны на правилах корреляции KUMA. Дополнительные сведения о правилах корреляции KUMA, включенных в комплект поставки, см. в разделе Правила корреляции.

Вы можете найти предустановленные плейбуки в разделе **Плейбуки**. Такие плейбуки помечаются тегом "**Predefined**" и префиксом [KL] в названии.

Обратите внимание, что вы не можете изменять параметры предустановленного плейбука, за исключением полей **Режим работы** и **Действие с запущенными экземплярами плейбука**. Если вы хотите изменить другие параметры предустановленного плейбука, вам нужно продублировать плейбук, а затем использовать его в качестве шаблона для создания пользовательского плейбука. Подробную информацию см. в разделе Настройка плейбуков:

Перед использованием предустановленных плейбуков в KUMA необходимо выполнить следующие действия:

- Настроить параметры правила обогащения для обогащения событий с выбранным типом **События** в качестве параметра **Тип источника**. Указать значения **VictimUserID** и **AttackerUserID** для параметра **Целевое поле**.
- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предустановленные плейбуки невозможно удалить.

Предустановленные плейбуки принадлежат родительскому тенанту и наследуются всеми дочерними тенантами.

[KL] P001 "Creation of executable files by office applications"

По лицензии EDR этот плейбук недоступен.

Этот плейбук содержит действие по реагированию Реагирование с помощью KASAP и может использоваться только в качестве шаблона. Если вы хотите запустить плейбук, нажмите на кнопку **Дублировать и изменить**. В открывшемся окне в действии **Назначить KASAP-группу** укажите идентификатор группы KASAP.

Перед использованием плейбука вам нужно настроить обогащение в KUMA, чтобы получить журнал событий Windows.

По умолчанию плейбук запускает действия по реагированию для всех пользователей в алерте. Если вы хотите, чтобы плейбук запускал действия по реагированию только для учетной записи атакуемого, вы можете сделать следующее:

1. В KUMA настройте параметры правила обогащения. Для обогащения событий, для которых выбран тип **События** в качестве параметра **Тип источника** указано значение **VictimUserID** в **Целевое поле**.

2. В действии **Назначить KASAP-группу** в поле **Активы** укажите `and .IsVictim` как показано ниже:

   ```
   [ alert.Assets[] | select(.Type == \"user\" and .IsVictim) | .ID]
   ```

Предустановленный плейбук **[KL]P001 "Creation of executable files by office applications"** позволяет предотвратить использование злоумышленником офисных приложений, например, для выполнения фишинговой атаки, когда пользователь открывает зараженный документ, а затем документ создает исполняемый файл и выполняет его.

Алерт, запускающий плейбук, создается в соответствии с правилом корреляции *Creation of executable files by office applications*. Это правило помогает обнаруживать создание файлов с подозрительными расширениями, такими как скрипты и исполняемые файлы, от имени офисных приложений.

Триггер плейбука содержит следующее выражение:

```
[.OriginalEvents[] | .ExternalID == "R350"] | any
```

Во время выполнения этот плейбук запускает следующие действия по реагированию:

1. Реагирование с помощью Active Directory и сброс паролей как атакующего, так и учетной записи атакуемого.

   > Если во время выполнения действия по реагированию возникает ошибка, плейбук прерывается.

2. Реагирование с помощью KASAP и присвоение учетной записи курса информационной безопасности.

   > Если во время выполнения действия по реагированию возникает ошибка, выполнение плейбука продолжается.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "resetLDAPPassword",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "action": {
```

```
                "function": {
                    "type": "assignKasapGroup",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}",
                    "params": {
                        "groupId": "SET KASAP GROUP ID"
                    }
                },
                "onError": "continue"
            }
        }
    ]
}
```

[KL] P002 "Windows Event Log was cleared"

По умолчанию этот плейбук работает в режиме **Ручной**. Не рекомендуется переключать этот плейбук в режим работы **Автоматический** или **Обучение**.

Перед использованием плейбука вам нужно выполнить в KUMA следующее:

- Настроить параметры правила обогащения для обогащения событий с выбранным типом События в качестве параметра Тип источника. Указать значение **AttackerUserID** для параметра **Целевое поле**.
- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предопределенный плейбук **[KL] P002 "Windows Event Log was cleared"** позволяет предотвратить очистку журнала событий Windows атакующим, так как журнал событий содержит данные телеметрии, достаточные для расследования злонамеренных действий атакующего.

Инцидент, запускающий плейбук, содержит один или несколько алертов, созданных в соответствии с правилом корреляции *Windows Event Log was cleared*. Это правило помогает определить, когда журналы событий Windows очищаются или удаляются с помощью утилиты wevutil, пользовательского интерфейса или команд PowerShell. Чтобы включить создание инцидента, вам необходимо настроить правила сегментации.

Триггер плейбука содержит следующее выражение:

```
[.Alerts[] | .OriginalEvents[] | .ExternalID  == "R050"] | any
```

Во время выполнения этот плейбук запускает действие по реагированию с помощью Active Directory и блокирует учетную запись атакующего.

Если во время выполнения действия по реагированию возникает ошибка, плейбук прерывается.

Если один или несколько алертов в инциденте генерируются другим правилом корреляции, плейбук не применяется к этим алертам.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${[ incident.Alerts[] | select(.OriginalEvents[] | .ExternalID == \"R050\") |
.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

[KL] P003 "Suspicious child process from wmiprvse.exe"

Перед использованием плейбука вам нужно выполнить в KUMA следующее:

- Настроить параметры правила обогащения для обогащения событий с выбранным типом События в качестве параметра Тип источника. Указать значение **AttackerUserID** для параметра **Целевое поле**.
- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предопределенный плейбук **[KL] P003 "Suspicious child process from wmiprvse.exe"** позволяет обнаруживать пары родительских и дочерних процессов, которые отклоняются от нормы и должны рассматриваться как подозрительные.

Алерт, который запускает плейбук, создается в соответствии с правилом корреляции *R297_Suspicious child process from wmiprvse.exe*. Это правило помогает обнаружить запуск подозрительных процессов от имени wmiprvse.exe.

Триггер плейбука содержит следующее выражение:

```
[.OriginalEvents[] | .ExternalID  == "R297"] | any
```

Во время выполнения этот плейбук запускает следующие действия по реагированию:

1. Действие по реагированию с помощью Active Directory с последующей блокировкой учетной записи атакующего.
2. Прерывание процесса на устройстве, зарегистрированном в алерте.
3. Запускается проверка на наличие вредоносных приложений, а затем выполняется полная проверка устройства, на котором обнаружен алерт.

> По умолчанию сетевые диски не проверяются во избежание перегрузки системы. Если вы хотите проверить сетевые диски, вам нужно продублировать этот плейбук, а затем в действии **Запустить поиск вредоносного ПО** включить переключатель **Проверить сетевые диски** или в редакторе кода для параметра `allowScanNetworkDrives` установить значение `true`.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "loop": {
                "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and
.DestinationProcessName != \"\")][] | .DestinationProcessName] }",
                "onError": "stop",
                "steps": [
                    {
                        "action": {
                            "function": {
                                "type": "killProcess",
                                "params": {
                                    "path": "${ .[0] }"
                                },
                                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                            }
                        }
                    }
                ]
            }
        },
        {
            "action": {
                "function": {
                    "type": "avScan",
                    "params": {
                        "scope": {
                            "area": "full",
                            "allowScanNetworkDrives": false
                        },
                        "wait": false
                    },
                    "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

Если во время выполнения любого действия по реагированию возникает ошибка, плейбук прерывается.

[KL] P004 "Sandbox Medium Detect"

Предустановленный плейбук **[KL] P004 "Sandbox Medium Detect"** создает правило для блокировки выполнения файлов, которым компонент Sandbox в результате анализа назначил уровень важности алерта **Средний**.

Триггер плейбука содержит следующее выражение:

```
"event.new and .Severity == \"medium\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

ResponseFunction, используемые плейбуком: `addFilePreventionRules`.

Во время выполнения в этом плейбуке используется реагирование Добавить правило запрета.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

[KL] P005 "Sandbox High Detect"

Предустановленный плейбук **[KL] P005 "Sandbox High Detect"** создает правило для блокировки выполнения файлов, которым компонент Sandbox в результате анализа назначил уровень важности алерта **Высокий**.

Триггер плейбука содержит следующее выражение:

```
"event.new and .Severity == \"high\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

ResponseFunction, используемые плейбуком: `addFilePreventionRules`.

Во время выполнения в этом плейбуке используется реагирование Добавить правило запрета.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

[KL] "Playbook for checking external IP addresses"

Предустановленный плейбук **[KL] "Playbook for checking external IP addresses"** запускается при обнаружении подключения к внешнему IP-адресу и инициирует процесс обогащения Kaspersky TIP. Если результаты обогащения показывают, что количество угроз превышает 80, для активов типа "host" запрашиваются данные для расследования (список процессов) и выполняется действие "Включить сетевую изоляцию".

Дополнительная информация о плейбуке.

- Для правильной работы плейбука нужно настроить интеграцию с Kaspersky TIP.
- Интеграция с Active Directory необходима для выполнения действий по блокировке учетных записей.
- Если результат обогащения показывает, что оценка угрозы ниже 80, плейбук прерывается.
- Выполнение плейбука будет остановлено, если на любом из шагов возникнет ошибка.
- Действие "Включить изоляцию сети" необходимо вручную подтвердить во время выполнения плейбука.

Триггер плейбука содержит следующее выражение:

```
"event.new and ([ .Alerts[] | .Observables[] | select(.Value | test("^(10\\.|172\\.(1[6-9]|2[0-9]|3[01])\\.|192\\.168\\.|127\\.)") | not) | .Value ] | length > 0)"
```

ResponseFunction используемые плейбуком: `iocsEnrichment, getForensics, netIsolateOn`.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "iocsEnrichment",
          "params": {
            "fullEnrichment": true,
            "observables": "${[ incident.Alerts[] | .Observables[] | {\"type\": .Type, \"value\": .Value } | select(.type==\"ip\" and (.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.)\") | not)) ] | unique_by(.value)}"
          }
        },
        "onError": "stop",
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        },
        "output": {
          "filter": "${.}",
          "action": "overwrite"
        }
      }
    },
    {
      "decision": {
        "conditions": [
          {
            "condition": "${\"${([.details.observableData[] | select(.status == \\\"ok\\\" and .ipObservableData.ipGeneralInfo.threatScore > 80)] | length > 0)}\"}",
            "name": "Condition 1",
```

```
            "steps": [
              {
                "decision": {
                  "conditions": [
                    {
                      "condition": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type == \"host\")) |
length > 0}",
                      "name": "alert has host(s)",
                      "steps": [
                        {
                          "action": {
                            "function": {
                              "type": "getForensics",
                              "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                              "params": {
                                "processes": {
                                  "collect": true
                                },
                                "autoruns": {
                                  "collect": false
                                }
                              }
                            },
                            "onError": "stop",
                            "timeout": {
                              "scheduleToCloseTimeout": "24h"
                            }
                          }
                        },
                        {
                          "action": {
                            "function": {
                              "type": "netIsolateOn",
                              "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                              "params": {
                                "exclusions": [],
                                "exclusionsConflictBehavior": "replace",
                                "isolationTimeoutSec": 28800
                              }
                            },
                            "onError": "stop",
                            "timeout": {
                              "scheduleToCloseTimeout": "24h"
                            },
                            "manualApprove": {
                              "timeout": "60m",
                              "emailNotifications": {
                                "enabled": true,
                                "delay": "10m"
                              }
                            }
                          }
                        }
                      ]
                    }
                  ]
                }
              }
            ]
          }
        ]
      }
    }
  ]
}
```

[KL] "Playbook for isolating a device where an infected file is detected"

Предустановленный плейбук **[KL] "Playbook for isolating a device where an infected file is detected"** изолирует устройство после обнаружения зараженного файла.

Плейбук не содержит триггер. Плейбук должен быть запущен вручную, и для этого нужно, чтобы пользователь выбрал контекст. Чтобы выполнить этот плейбук, вам нужно установить флажок **Выберите целевые объекты перед запуском плейбуков** и выбрать активы инцидентов и наблюдаемые объекты, для которых он будет выполняться.

Для каждого выбранного типа хеша наблюдаемого объекта выполняются следующие действия:

1. Получение файла из выбранного актива.
2. Отправка полученного файла на проверку.
   - Если во время проверки возникает ошибка, выполнение плейбука прерывается.
   - Если проверка завершена и угрозы не обнаружены, выполнение плейбука прерывается.
   - Если проверка завершена и угроза обнаружена:
     - На всех выбранных устройствах включается сетевая изоляция.
     - Правило запрета на основе хеша добавляется ко всем устройствам в тенанте.

Дополнительная информация о плейбуке.

- Если на шагах по добавлению правил запрета для включения сетевой изоляции возникает ошибка, выполнение плейбука прерывается, во всех других случаях оно будет продолжаться.
- Действия "Включить сетевую изоляцию" и "Добавить правило запрета" необходимо вручную подтвердить во время выполнения плейбука.

ResponseFunction используется плейбуком: `getFile`, `serverScan`, `addCommentToIncident`, `addFilePreventionRules`, `netIsolateOn`.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "decision": {
        "conditions": [
          {
            "condition": "${((.input.assets // []) | length) > 0 and ([.input.observables[] | select(.type == \"md5\" or .type == \"sha256\" and .value != null and .value != \"\")] | length) > 0}",
            "name": "has input data",
            "steps": [
              {
                "loop": {
                  "input": "${[(.input.observables | map(select(.type == \"md5\" or .type == \"sha256\") | select(.value != null and .value != \"\") | .value))[] as $hash | [incident.Alerts[] | .Observables[]? | select((.Type == \"md5\" or .Type == \"sha256\") and .Value == $hash and .Details != \"\")][0] | {\"path\": .Details,\"hash\":.Value}]}",
                  "steps": [
                    {
                      "decision": {
                        "conditions": [
                          {
                            "condition": "${.[0].path? | length > 0}",
                            "name": "hash with path",
                            "steps": [
                              {
                                "updateData": {
                                  "action": "merge",
```

```
                                "filter": "${.[0]}"
                              }
                            },
                            {
                              "action": {
                                "function": {
                                  "type": "getFile",
                                  "asset": "${([incident.Alerts[] | .Assets[]? | select(.Type == \"host\")]
[0].ID // (.assets[0] // \"\"))}",
                                  "params": {
                                    "path": "${.path}"
                                  }
                                },
                                "onError": "continue",
                                "timeout": {
                                  "scheduleToCloseTimeout": "24h"
                                },
                                "output": {
                                  "action": "merge",
                                  "filter": "${{\"fileID\": (.details[0].details.file.id // null),
\"scanResult\": null}}"
                                }
                              }
                            },
                            {
                              "decision": {
                                "conditions": [
                                  {
                                    "condition": "${.fileID != null and .fileID != \"\"}",
                                    "name": "fileID exists",
                                    "steps": [
                                      {
                                        "action": {
                                          "function": {
                                            "type": "serverScan",
                                            "params": {
                                              "file": {
                                                "id": "${.fileID}"
                                              }
                                            }
                                          },
                                          "onError": "continue",
                                          "timeout": {
                                            "scheduleToCloseTimeout": "24h"
                                          },
                                          "output": {
                                            "action": "merge",
                                            "filter": "${{\"scanResult\": .}}"
                                          }
                                        }
                                      },
                                      {
                                        "decision": {
                                          "conditions": [
                                            {
                                              "condition": "${.scanResult != null and (.scanResult.resultCode ==
\"error\" or .scanResult.resultCode == null)}",
                                              "name": "scan error",
                                              "steps": [
                                                {
                                                  "action": {
                                                    "function": {
                                                      "type": "addCommentToIncident",
                                                      "params": {
                                                        "text": "${\"[DEBUG scan ERROR] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \" | errorCode: \" +
(.scanResult.result.errorCode // \"null\") + \" | internalCode: \" + (.scanResult.result.internalCode // \"null\")
+ \"\\noriginalError: \" + (.scanResult.result.originalError // \"null\")}"
                                                      }
                                                    },
                                                    "onError": "continue",
                                                    "timeout": {
                                                      "scheduleToCloseTimeout": "24h"
                                                    }
                                                  }
                                                }
                                              ]
                                            },
                                            {
                                              "condition": "${.scanResult != null and .scanResult.resultCode ==
\"success\"}",
                                              "name": "scan success",
```

```
                                                    "steps": [
                                                      {
                                                        "action": {
                                                          "function": {
                                                            "type": "addCommentToIncident",
                                                            "params": {
                                                              "text": "${\"[DEBUG scan] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \"\\nresult: \" + ({\"fileID\": .fileID,
\"resultCode\": .scanResult.resultCode, \"technologies\": .scanResult.details.scanResult.technologies} |
tostring)}"
                                                            }
                                                          },
                                                          "onError": "continue",
                                                          "timeout": {
                                                            "scheduleToCloseTimeout": "24h"
                                                          }
                                                        }
                                                      },
                                                      {
                                                        "decision": {
                                                          "conditions": [
                                                            {
                                                              "condition":
"${[.scanResult.details.scanResult.technologies[] | .result] | contains([\"Infected\"])}",
                                                              "name": "infected",
                                                              "steps": [
                                                                {
                                                                    "action": {
                                                                        "function": {
                                                                          "type": "addFilePreventionRules",
                                                                          "assets":[
                                                                            "selector": "execution-tenant"
                                                                          },
                                                                          "params": {
                                                                            "files": "${[.hash]}"
                                                                          }
                                                                        },
                                                                        "onError": "stop",
                                                                        "timeout": {
                                                                          "scheduleToCloseTimeout": "24h"
                                                                        },
                                                                        "manualApprove": true
                                                                    }
                                                                },
                                                                {
                                                                  "updateData": {
                                                                    "action": "overwrite",
                                                                    "filter": "${{\"isInfected\": true}}"
                                                                  }
                                                                }
                                                              ]
                                                            }
                                                          ]
                                                        }
                                                      }
                                                    ]
                                                  }
                                                ]
                                              }
                                            ]
                                          }
                                        ]
                                      }
                                    ]
                                  }
                                ]
                              }
                            ]
                          }
                        ]
                      }
                    ],
                    "onError": "continue",
                    "batchSize": 1,
                    "aggregate": "${.}",
                    "output": {
                      "filter": "${{\"scanResult\": .}}"
                    }
                  }
                },
                {
                  "decision": {
                    "conditions": [
```

```
                    {
                      "condition": "${.scanResult | map(.isInfected) | any}",
                      "name": "isInfected",
                      "steps": [
                        {
                          "action": {
                            "function": {
                              "type": "netIsolateOn",
                              "assets": "${.input.assets | map(select(.Type == \"host\") | .ID)}",
                              "params": {
                                "exclusions": [],
                                "exclusionsConflictBehavior": "replace",
                                "isolationTimeoutSec": 28800
                              }
                            },
                            "onError": "stop",
                            "timeout": {
                              "scheduleToCloseTimeout": "24h"
                            }
                          }
                        }
                      ]
                    }
                  ]
                }
              }
            ]
          }
        ]
      }
    }
  ]
}
```

[KL] "Playbook for isolating a device where an infected file is detected"

Предустановленный плейбук **[KL] "Playbook for isolating a device where an infected file is detected"** изолирует устройство после обнаружения зараженного файла.

Плейбук не содержит триггер. Плейбук должен быть запущен вручную, и для этого нужно, чтобы пользователь выбрал контекст. Чтобы выполнить этот плейбук, вам нужно установить флажок **Выберите целевые объекты перед запуском плейбуков** и выбрать активы инцидентов и наблюдаемые объекты, для которых он будет выполняться.

Для каждого выбранного типа хеша наблюдаемого объекта выполняются следующие действия:

1. Получение файла из выбранного актива.
2. Отправка полученного файла на проверку.
   - Если во время проверки возникает ошибка, выполнение плейбука прерывается.
   - Если проверка завершена и угрозы не обнаружены, выполнение плейбука прерывается.
   - Если проверка завершена и угроза обнаружена:
     - На всех выбранных устройствах включается сетевая изоляция.
     - Правило запрета на основе хеша добавляется ко всем устройствам в тенанте.

Дополнительная информация о плейбуке.

- Если на шагах по добавлению правил запрета для включения сетевой изоляции возникает ошибка, выполнение плейбука прерывается, во всех других случаях оно будет продолжаться.

- Действия "Включить сетевую изоляцию" и "Добавить правило запрета" необходимо вручную подтвердить во время выполнения плейбука.

ResponseFunction используется плейбуком: `getFile`, `serverScan`, `addCommentToIncident`, `addFilePreventionRules`, `netIsolateOn`.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "decision": {
        "conditions": [
          {
            "condition": "${((.input.assets // []) | length) > 0 and ([.input.observables[] | select(.type == \"md5\" or .type == \"sha256\" and .value != null and .value != \"\")] | length) > 0}",
            "name": "has input data",
            "steps": [
              {
                "loop": {
                  "input": "${[(.input.observables | map(select(.type == \"md5\" or .type == \"sha256\") | select(.value != null and .value != \"\") | .value))[] as $hash | [incident.Alerts[] | .Observables[]? | select((.Type == \"md5\" or .Type == \"sha256\") and .Value == $hash and .Details != \"\")][0] | {\"path\": .Details,\"hash\":.Value}]}",
                  "steps": [
                    {
                      "decision": {
                        "conditions": [
                          {
                            "condition": "${.[0].path? | length > 0}",
                            "name": "hash with path",
                            "steps": [
                              {
                                "updateData": {
                                  "action": "merge",
                                  "filter": "${.[0]}"
                                }
                              },
                              {
                                "action": {
                                  "function": {
                                    "type": "getFile",
                                    "asset": "${([incident.Alerts[] | .Assets[]? | select(.Type == \"host\")][0].ID // (.assets[0] // \"\"))}",
                                    "params": {
                                      "path": "${.path}"
                                    }
                                  },
                                  "onError": "continue",
                                  "timeout": {
                                    "scheduleToCloseTimeout": "24h"
                                  },
                                  "output": {
                                    "action": "merge",
                                    "filter": "${{\"fileID\": (.details[0].details.file.id // null), \"scanResult\": null}}"
                                  }
                                }
                              },
                              {
                                "decision": {
                                  "conditions": [
                                    {
                                      "condition": "${.fileID != null and .fileID != \"\"}",
                                      "name": "fileID exists",
                                      "steps": [
```

```
                                        {
                                          "action": {
                                            "function": {
                                              "type": "serverScan",
                                              "params": {
                                                "file": {
                                                  "id": "${.fileID}"
                                                }
                                              }
                                            },
                                            "onError": "continue",
                                            "timeout": {
                                              "scheduleToCloseTimeout": "24h"
                                            },
                                            "output": {
                                              "action": "merge",
                                              "filter": "${{\"scanResult\": .}}"
                                            }
                                          }
                                        },
                                        {
                                          "decision": {
                                            "conditions": [
                                              {
                                                "condition": "${.scanResult != null and (.scanResult.resultCode ==
\"error\" or .scanResult.resultCode == null)}",
                                                "name": "scan error",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan ERROR] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \" | errorCode: \" +
(.scanResult.result.errorCode // \"null\") + \" | internalCode: \" + (.scanResult.result.internalCode // \"null\")
+ \"\\noriginalError: \" + (.scanResult.result.originalError // \"null\")}"
                                                        }
                                                      },
                                                      "onError": "continue",
                                                      "timeout": {
                                                        "scheduleToCloseTimeout": "24h"
                                                      }
                                                    }
                                                  }
                                                ]
                                              },
                                              {
                                                "condition": "${.scanResult != null and .scanResult.resultCode ==
\"success\"}",
                                                "name": "scan success",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \"\\nresult: \" + ({\"fileID\": .fileID,
\"resultCode\": .scanResult.resultCode, \"technologies\": .scanResult.details.scanResult.technologies} |
tostring)}"
                                                        }
                                                      },
                                                      "onError": "continue",
                                                      "timeout": {
                                                        "scheduleToCloseTimeout": "24h"
                                                      }
                                                    }
                                                  },
                                                  {
                                                    "decision": {
                                                      "conditions": [
                                                        {
                                                          "condition":
"${[.scanResult.details.scanResult.technologies[] | .result] | contains([\"Infected\"])}",
                                                          "name": "infected",
                                                          "steps": [
                                                            {
                                                                "action": {
                                                                    "function": {
                                                                      "type": "addFilePreventionRules",
                                                                      "assets":[
```

```
                                                                                "selector": "execution-tenant"
                                                                              },
                                                                              "params": {
                                                                                "files": "${[.hash]}"
                                                                              }
                                                                            },
                                                                            "onError": "stop",
                                                                            "timeout": {
                                                                              "scheduleToCloseTimeout": "24h"
                                                                            },
                                                                            "manualApprove": true
                                                                          }
                                                                        },
                                                                        {
                                                                          "updateData": {
                                                                            "action": "overwrite",
                                                                            "filter": "${{\"isInfected\": true}}"
                                                                          }
                                                                        }
                                                                      ]
                                                                    }
                                                                  ]
                                                                }
                                                              }
                                                            ]
                                                          }
                                                        ]
                                                      }
                                                    ]
                                                  }
                                                ]
                                              }
                                            ]
                                          }
                                        ]
                                      }
                                    ]
                                  }
                                ]
                                "onError": "continue",
                                "batchSize": 1,
                                "aggregate": "${.}",
                                "output": {
                                  "filter": "${{\"scanResult\": .}}"
                                }
                              }
                            },
                            {
                              "decision": {
                                "conditions": [
                                  {
                                    "condition": "${.scanResult | map(.isInfected) | any}",
                                    "name": "isInfected",
                                    "steps": [
                                      {
                                        "action": {
                                          "function": {
                                            "type": "netIsolateOn",
                                            "assets": "${.input.assets | map(select(.Type == \"host\") | .ID)}",
                                            "params": {
                                              "exclusions": [],
                                              "exclusionsConflictBehavior": "replace",
                                              "isolationTimeoutSec": 28800
                                            }
                                          },
                                          "onError": "stop",
                                          "timeout": {
                                            "scheduleToCloseTimeout": "24h"
                                          }
                                        }
                                      }
                                    ]
                                  }
                                ]
                              }
                            }
                          ]
                        }
                      ]
                    }
                  }
```

```
  ]
}
```

[KL][EDR] "Delete malicious files transferred to the host from alert"

Предустановленный плейбук **[KL][EDR] Delete malicious files transferred to the host from alert** предназначен для автоматического реагирования на обнаружение вредоносных файлов, которые используются для доставки на устройство дополнительного вредоносного ПО. При обнаружении активности, связанной с техникой T1105 (Ingress Tool Transfer), плейбук удаляет такой файл с устройства, чтобы предотвратить его дальнейшее использование.

Область применения плейбука – алерты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any(.S.KL_EventType == "File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert,
.SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == "t1105")))))] | any)"
```

ResponseFunction, используемая плейбуком: `deleteFile`.

Во время выполнения плейбук использует реагирование **Удалить файл**.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and (.FileFullname //
\"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == \"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
}
```

[KL][EDR] "Delete malicious files transferred to the host from incident"

Предустановленный плейбук **[KL][EDR] Delete malicious files transferred to the host from incident** предназначен для автоматического реагирования на обнаружение вредоносных файлов, которые используются для доставки на устройство дополнительного вредоносного ПО. Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении активности, связанной с техникой T1105 (Ingress Tool Transfer), плейбук удаляет такой файл с устройства, чтобы предотвратить его дальнейшее использование.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(.S.KL_EventType ==
"File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0]
and .[1] == "t1105")))) ] | any)"
```

ResponseFunction, используемая плейбуком: `deleteFile`.

Во время выполнения плейбук использует реагирование **Удалить файл**.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and
(.FileFullname // \"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] ==
\"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
}
```

[KL][EDR] "Isolate host when Discovery activity is detected from alert"

Предустановленный плейбук **[KL][EDR] Isolate host when Discovery activity is detected from alert** предназначен для автоматического реагирования на активность по сбору информации об устройстве и его окружении. При обнаружении такой активности плейбук включает сетевую изоляцию устройства, чтобы предотвратить дальнейшие действия злоумышленника во время расследования.

Область применения плейбука – алерты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.Rules // [] |
select(any(.Name == "Discovery_activity_on_the_host"))] | any)"
```

ResponseFunction, используемая плейбуком: `netIsolateOn`.

Во время выполнения плейбук использует реагирование **Включить сетевую изоляцию**. Данное реагирование включает сетевую изоляцию устройства на 8 часов. Для включения сетевой изоляции требуется подтверждение пользователя.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] "Isolate host when Discovery activity is detected from incident"

Предустановленный плейбук **[KL][EDR] Isolate host when Discovery activity is detected from incident** предназначен для автоматического реагирования на активность по сбору информации об устройстве и его окружении. Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении такой активности включает сетевую изоляцию устройства, чтобы предотвратить дальнейшие действия злоумышленника во время расследования.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .Rules // [] | select(any(.Name ==
"Discovery_activity_on_the_host")) ] | any)"
```

ResponseFunction, используемая плейбуком: `netIsolateOn`.

Во время выполнения плейбук использует реагирование **Включить сетевую изоляцию**. Данное реагирование включает сетевую изоляцию устройства на 8 часов. Для включения сетевой изоляции требуется подтверждение пользователя.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | select(.Rules | any(.Name == \"Discovery_activity_on_the_host\")) |
.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] "Isolate host when Exfiltration activity is detected"

Предустановленный плейбук **[KL][EDR] Isolate host when Exfiltration activity is detected** предназначен для автоматического реагирования на попытки несанкционированной передачи данных с устройства и соединения с инфраструктурой управления злоумышленника (C2). Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении такой активности включает сетевую изоляцию устройства, чтобы предотвратить дальнейшую передачу данных и вредоносную активность.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | map(select(.[0]) | .[1]) | any(. as $v | ["not_standard_directory_archive",
"compress_data_for_exfiltration_via_archive"] | index($v)) and any(. as $v | ["lolc2_connection_activity_network",
"lolc2_connection_activity_dns", "network_connection_to_cloud_storage_win"] | index($v)))) ] | any)"
```

ResponseFunction, используемая плейбуком: `netIsolateOn`.

Во время выполнения плейбук использует реагирование **Включить сетевую изоляцию**. Данное реагирование включает сетевую изоляцию устройства на 8 часов. Для включения сетевой изоляции требуется подтверждение пользователя.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | map(select(.[0]) | .[1]) | any(. as $v | [\"not_standard_directory_archive\",
\"compress_data_for_exfiltration_via_archive\"] | index($v)) and any(. as $v |
[\"lolc2_connection_activity_network\", \"lolc2_connection_activity_dns\",
\"network_connection_to_cloud_storage_win\"] | index($v))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] "Isolate host when reverse shell activity is detected from alert"

Предустановленный плейбук **[KL][EDR] Isolate host when reverse shell activity is detected from alert** предназначен для автоматического реагирования на признаки использования обратной оболочки (reverse shell) на устройстве. При обнаружении такой активности плейбук включает сетевую изоляцию устройства, чтобы предотвратить удаленное управление устройством злоумышленником.

Область применения плейбука – алерты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell",
"invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname))))) ]
| any)"
```

ResponseFunction, используемая плейбуком: `netIsolateOn`.

Во время выполнения плейбук использует реагирование **Включить сетевую изоляцию**. Данное реагирование включает сетевую изоляцию устройства на 8 часов. Для включения сетевой изоляции требуется подтверждение пользователя.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1]
as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] "Isolate host when reverse shell activity is detected from incident"

Предустановленный плейбук **[KL][EDR] Isolate host when reverse shell activity is detected from incident** предназначен для автоматического реагирования на признаки использования обратной оболочки (reverse shell) на устройстве. Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении такой активности плейбук включает сетевую изоляцию устройства, чтобы предотвратить удаленное управление устройством злоумышленником.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . == "incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell", "invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname)))))] | any)"

ResponseFunction, используемая плейбуком: `netIsolateOn`.

Во время выполнения плейбук использует реагирование **Включить сетевую изоляцию**. Данное реагирование включает сетевую изоляцию устройства на 8 часов. Для включения сетевой изоляции требуется подтверждение пользователя.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
```

```
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] "Mitigate malicious activity from email attachments from alert"

Предустановленный плейбук **[KL][EDR] Mitigate malicious activity from email attachments from alert** предназначен для автоматического реагирования на вредоносную активность, связанную с файлами, полученными по электронной почте. При обнаружении такой активности на устройстве плейбук завершает связанный с вредоносным файлом процесс и удаляет этот файл с устройства.

Область применения плейбука – алерты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([ .OriginalEvents //
[] | select(any(. as $event | $event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null
then $event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

ResponseFunction, используемые плейбуком: `killProcess`, `deleteFile`.

Во время выполнения плейбук использует следующие реагирования:

- Завершить процесс

  > Если завершить процесс не удалось, выполнение плейбука продолжается.

- Удалить файл

События алерта могут относиться к разным устройствам и вредоносным файлам. Плейбук запускает реагирования отдельно для каждого подходящего события. Если в алерте нет подходящих событий, выполнение плейбука завершается.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
```

```
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or .ParentFileName == \"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname | test(\"\\\\w\\\\:\\\\\\\\\\\\\\\")))  ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
}
```

[KL][EDR] "Mitigate malicious activity from email attachments from incident"

Предустановленный плейбук **[KL][EDR] Mitigate malicious activity from email attachments from incident** предназначен для автоматического реагирования на вредоносную активность, связанную с файлами, полученными по электронной почте. Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении вредоносной активности на устройстве завершает связанный с вредоносным файлом процесс и удаляет этот файл с устройства.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . == "incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(. as $event | $event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null then $event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

ResponseFunction, используемые плейбуком: `killProcess`, `deleteFile`.

Во время выполнения плейбук использует следующие реагирования:

- Завершить процесс

  Если завершить процесс не удалось, выполнение плейбука продолжается.

- Удалить файл

События алерта могут относиться к разным устройствам и вредоносным файлам. Плейбук запускает реагирования отдельно для каждого подходящего события. Если в алерте нет подходящих событий, выполнение плейбука завершается.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or
.ParentFileName == \"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname |
test(\"\\\\w\\\\:\\\\\\\\\\\")) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
  }
```

[KL][EDR] "Mitigate memory dumping activity from alert"

Предустановленный плейбук **[KL][EDR] Mitigate memory dumping activity from alert** предназначен для автоматического реагирования на создание дампов памяти, которые могут использоваться для получения учетных данных и другой конфиденциальной информации. При обнаружении такой активности на устройстве плейбук завершает процесс, создавший дамп памяти, и удаляет созданные этим процессом файлы.

Область применения плейбука – алерты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["createdump_lolbin_execution_process", "credentials_dumping_tools_epp",
"credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] | any)"
```

ResponseFunction, используемые плейбуком: `killProcess`, `deleteFile`.

Во время выполнения плейбук использует следующие реагирования:

- Завершить процесс

  > Если завершить процесс не удалось, выполнение плейбука продолжается.

- Удалить файл

События алерта могут относиться к разным устройствам и вредоносным файлам. Плейбук запускает реагирования отдельно для каждого подходящего события. Если в алерте нет подходящих событий, выполнение плейбука завершается.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any( .[1]
as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\", \"credentials_dumping_tools_epp\",
\"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ] }",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
```

```
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```

[KL][EDR] "Mitigate memory dumping activity from incident"

Предустановленный плейбук **[KL][EDR]Mitigate memory dumping activity from incident** предназначен для автоматического реагирования на создание дампов памяти, которые могут использоваться для получения учетных данных и другой конфиденциальной информации. Плейбук обрабатывает алерты, связанные с инцидентом, и при обнаружении такой активности на устройстве завершает процесс, создавший дамп памяти, и удаляет созданные этим процессом файлы.

Область применения плейбука – инциденты.

Триггер плейбука содержит следующее выражение:

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["createdump_lolbin_execution_process",
"credentials_dumping_tools_epp", "credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] |
any)"
```

ResponseFunction, используемые плейбуком: `killProcess`, `deleteFile`.

Во время выполнения плейбук использует следующие реагирования:

- Завершить процесс

  Если завершить процесс не удалось, выполнение плейбука продолжается.

- Удалить файл

События алерта могут относиться к разным устройствам и вредоносным файлам. Плейбук запускает реагирования отдельно для каждого подходящего события. Если в алерте нет подходящих событий, выполнение плейбука завершается.

Алгоритм плейбука содержит следующую последовательность действий по реагированию:

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
```

```
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\",
\"credentials_dumping_tools_epp\", \"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ]
}",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```

Триггер плейбука

Триггер плейбука – это фильтр, позволяющий выбрать алерты или инциденты, для которых необходимо запустить плейбук. Фильтр (триггер) применяется к каждому объекту (алерту или инциденту) индивидуально и принимает одно значение: `true` или `false`. Триггер состоит из выражений на языке jq, обрабатывающих структурированные данные в формате JSON. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

В Kaspersky EDR Expert используется gojq. Это реализация jq, написанная на языке go, которая имеет следующие отличия от jq:

- Математические функции реализованы более удобным образом.
- В сообщениях об ошибках точно указано место, где нужно исправить ваш запрос.
- Целочисленные вычисления более точные.
- В gojq улучшены функции, которые некорректно работают в jq.

Дополнительные сведения о различиях между gojq и jq см. на сайте GitHub.

Как написать триггер

Вы можете написать триггер в блоке **Триггер** визуального редактора при создании или изменении плейбука.

В зависимости от того, какой параметр вы выбрали в списке **Область действия** при создании или изменении плейбука, используется модель данных алерта или модель данных инцидента.

> Названия параметров в триггере плейбука должны быть такими же, как в модели данных. Обратите внимание, что элементы выражений jq чувствительны к регистру.

> Чтобы избежать перегрузки системы не рекомендуется указывать в триггере данные `OriginalEvents, Observables, Extra` и `Alerts`.

Когда вы начнете писать триггер, могут отобразится следующие предложения:

- названия функций;
- особые значения;
- поля, которые указаны как идентификаторы объекта в соответствии с моделью данных.

Подходящие значения фильтруются и отображаются в списке предложений, когда вы начинаете писать триггер. Для удобства некоторые предложения содержат строку поиска. Например, если вы хотите указать идентификатор типа инцидента или идентификатор статуса инцидента, вы можете выполнить поиск соответствующей записи по имени и этот идентификатор будет указан в триггере.

> Обратите внимание, что стандартные статусы (*Новый* и *Закрыт*) имеют одинаковые идентификаторы в разных рабочих процессах. Это означает, что триггер будет запускаться для всех инцидентов с указанным идентификатором статуса. Чтобы ограничить количество инцидентов, для которых будет запущен плейбук, в триггере вам нужно указать идентификатор статуса инцидента и тип инцидента.

Язык jq также обеспечивает подсветку синтаксиса и проверку выражений jq. Если в триггере есть недопустимые выражения, вы не можете сохранить плейбук.

При написании триггера используются базовые синтаксические правила.

Чтобы обратиться к свойствам структуры, вам нужно использовать точку "`.`" и указать атрибут, например:

- `.MITRETactics[]` – для просмотра массива тактик MITRE, связанных со всеми сработавшими IOA-правилами в алерте.
- `.MITRETactics[0]` – для просмотра первого элемента из массива тактик MITRE.

Чтобы обратиться к дочерним свойствам, вы можете использовать вертикальную черту (|) или ту же комбинацию без вертикальной черты, например:

- `.Assignee.Name` – выражение выводит имя пользователя, которому назначен алерт.
- `.MITRETactics[0].ID` или `.MITRETactics[0] | .ID` – выражение выводит идентификатор первой тактики MITRE.

Чтобы получить значение, необходимо использовать следующие операторы: ==, >, <, >=, <=, !=, например:

- `.Assignee.Name == "user"` – выражение возвращает значение `true`, если алерт назначен пользователю.
- `(.Severity == "high") and (.DetectSource == "KES")` – выражение возвращает значение `true`, если уровень важности алерта высокий и источником данных является Kaspersky Endpoint Security.
- `[ .DetectionTechnologies[] | . == "IOC" ] | any` – выражение возвращает значение `true`, если срабатывает технология обнаружения IOC.
- `.DetectionTechnologies | length > 1` – выражение возвращает значение `true`, если срабатывает более одной технологии обнаружения.

Для перечисления значений в массиве объектов можно использовать метод `any`, например:

- `[.Assets[] | .Name == "W21H2-X64-3160"] | any` – выражение фильтрует алерты, в которых любой элемент массива `Assets` имеет значение `W21H2-X64-3160` в поле `Name`.
- `[.Observables[] | .Value == "127.0.0.1"] | any` – выражение фильтрует алерты, в которых любой элемент массива `Observables` имеет значение `127.0.0.1` в поле `Value`.
- `[.Assets[].ID]` – для вывода массива идентификаторов.
- `[.Assets[] | select(.AttackerOrVictim=="attacker") | .ID]` – для отображения массива идентификаторов активов, отфильтрованных по полю `AttackerOrVictim`.

Если вы хотите повторно использовать вычисления, укажите переменную с помощью `$`. Например, выражение `event.manual != true as $not_manual | [ .DetectionTechnologies[] | . == "IOC" ] | any and $not_manual` определяет и использует переменную `$not_manual`, которая содержит флаг, показывающий, внесено ли изменение вручную или нет.

Для работы с датами вы можете использовать следующие функции:

- `now` – чтобы получить текущее время Unix в секундах, например, `now == 1690541520.537496`.
- `todate` – чтобы конвертировать текущее время Unix в строку даты, например, `now | todate == "2023-07-28T10:47:36Z".`
- `fromdate` – чтобы преобразовать дату в секунды, например:
  - `.CreatedAt | split(".")[0] + "Z"` – эта команда удаляет миллисекунды и преобразует строку в формат 2023-07-15T07:49:51Z.
  - `(.CreatedAt | split(".")[0] + "Z") | fromdate == 1689407391` – преобразование в секунды завершено.

Jq использует итераторы – интерфейс, который обеспечивает доступ к элементам набора, например к массиву, и позволяет вам перемещаться по ним. Итераторы всегда являются результатом расчета. Разница в количестве элементов, которые содержит итератор. В Kaspersky EDR Expert итератор должен иметь только один элемент. Остальные случаи считаются ошибкой.

Чтобы написать правильный триггер, вам нужно заключить итератор в квадратные скобки (`[...]`). Например, триггер `.DetectionTechnologies[] == "IOC"` вызовет ошибку, так как возвращает итератор с двумя элементами. Правильный триггер должен иметь следующий вид: `[ .DetectionTechnologies == "IOC" ] | any`, где сначала вам нужно использовать `[]`, чтобы обернуть результат сравнения в массив, а затем обработать его с помощью метода `any`, который возвращает значение `true`, если хотя бы один элемент массива `true`. Иначе возвращается `false`.

Когда запускается триггер

Поиск подходящего плейбука начинается при возникновении одного из следующих триггерных событий:

- Новый алерт/инцидент создан.
- Любое поле активного алерта/инцидента изменилось.
- При создании или изменении плейбука пользователь выбрал **Запустите плейбук для всех совпадающих алертов или инцидентов. Обратите внимание, что система может быть перегружена**.

Поддерживаются следующие типы событий изменения алертов:

- Назначение или удаление аналитика.
- Изменение статуса алерта.
- Изменение базовых событий.
- Связывание или удаление связи алерта с инцидентом.
- Изменение значения в поле `ExternalReference`.

Поддерживаются следующие типы событий изменения инцидента:

- Назначение или удаление аналитика.
- Изменение статуса инцидента.
- Изменение базовых событий.
- Связывание или удаление связи алерта с инцидентом.
- Изменение названия инцидента.
- Изменение описания инцидента.
- Изменение приоритета инцидента.

- Изменение значения в поле `ExternalReference`.

- Объединение инцидентов.

Структура алерта/инцидента не содержит данных об изменении алерта/инцидента. Эти данные передаются в дополнительной информации. Если в триггере плейбука вы хотите сослаться на изменения, используйте функцию события без аргументов.

По умолчанию изменения, внесенные вручную в детали алерта или инцидента, игнорируются. Если вы хотите, чтобы плейбук запускался для изменений выполненных вручную, вы должны использовать функцию `event.manual` в триггере, например:

- `event.manual and ([ event.updateOperations[] | . == "alertReopened" ] | any)` – триггер срабатывает, только если алерт повторно открывается вручную.

- `[ event.updateOperations[] | . == "alertLinkedWithIncidentBySystem" ] | any` – триггер срабатывает, только если алерт автоматически связывается с инцидентом.

- `event.manual != null and (([ event.updateOperations[] | . == "alertChangedToNew" ] | any) | not)` – триггер срабатывает, если статус алерта изменяется на любой статус, кроме *Новый*, вручную или автоматически.

- `event == null and .Status == "inIncident"` – триггер работает для всех алертов со статусом *В инциденте*, но только при изменении плейбука, а не алерта.

При необходимости вы можете протестировать примеры jq-выражений, применить фильтры и просмотреть результаты на сервисе Jq playground.

Алгоритм плейбука

Kaspersky EDR Expert позволяет вам реагировать на алерты и инциденты вручную или автоматически с использованием плейбуков. Реагирование на алерты или инциденты может состоять не из одного действия, а из целого набора шагов и параметров. Эти шаги зависят от указанных условий, данных об алерте или инциденте, а также результатов предыдущих действий по реагированию.

Алгоритм плейбука позволяет вам указать последовательность действий по реагированию, необходимые условия и требуемое воздействие на целевые объекты в формате JSON. Шаги алгоритма плейбука выполняются последовательно. Вы можете указать алгоритм плейбука при создании или изменении плейбука.

После запуска, плейбук получает все данные алертов или инцидентов и помещает их в глобальные данные. Плейбук использует следующие данные:

- Глобальные данные.

  Глобальные данные доступны для чтения на любом этапе плейбука. Глобальные данные содержат информацию об алерте или инциденте, для которого был запущен плейбук.

  > Вы не можете изменить глобальные данные с помощью плейбука или изменяя данные алерта или инцидента. Глобальные данные остаются неизменными в течение всего времени существования экземпляра плейбука.

- Операционные данные.

  Операционные данные передаются между шагами плейбука. Вы можете управлять операционными данными с помощью выражений jq, которые указаны в параметрах `input` и `output`.

- Локальные данные.

  Локальные данные ограничены определенным шагом. Вы можете управлять локальными данными, используя параметры `input` (создание локальных данных) и `output` (создание операционных данных из локальных данных).

Как написать алгоритм

Алгоритм плейбука описывается в формате JSON и состоит из двух основных частей:

- Общая информация о плейбуке:
  - Название (`name`).
  - Описание (`description`).
  - Источник (`inputType`).
  - Преобразование входных данных плейбука (`input`).
  - Преобразование выходных данных плейбука (`output`).
  - Время ожидания выполнения плейбука (`playbookRunTimeout`).
  - Политики времени ожидания, которые могут быть применены на определенных шагах (`timeouts`).
  - Версия плейбука (`version`).
  - Версия схемы DSL (`dslSpecVersion`).
  - Версия схемы действия по реагированию (`actionsSpecVersion`).
- Шаги выполнения плейбука (`executionFlow`).

Следующие параметры нужны при написании алгоритма:

- `dslSpecVersion`. Требуемое значение: 1.1.0.
- `actionsSpecVersion`
- `version`
- `executionFlow` (хотя бы один шаг выполнения).

> Каждый шаг выполнения имеет свои обязательные поля.

Если вы попытаетесь сохранить плейбук без заполнения обязательных полей, отобразится ошибка.

Алгоритм плейбука чувствителен к регистру. Чтобы использовать данные активов из алерта, вам нужно использовать параметр `Assets` с заглавной буквы. Например: `alert.Assets[]`. Чтобы использовать данные активов во входных данных при запуске плейбука вручную для целевых объектов, не используйте заглавные буквы в параметре `assets`. Например: `.input.assets[]`.

В зависимости от выбранной вами области действия при создании или изменении плейбука вы можете использовать в выражениях, написанных на jq-языке, модель данных алерта или модель данных инцидента. Для этого напишите выражения со значением `alert` или `incident` (не используйте точку `"."` в начале значения). Например:

```
"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
```

Вы можете использовать данные алерта или инцидента в выражении jq на любом шаге выполнения. Данные алерта или инцидента доступны только в режиме чтения. Эти данные не изменяются во время работы плейбука. Если данные алерта или инцидента изменились после запуска плейбука, это не повлияет на выполнение плейбука.

Вы также можете использовать выражения jq при использовании данных плейбука в алгоритме. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

> Если вы используете кавычки в выражении jq, вам нужно экранировать эти знаки обратными косыми чертами. Например: `"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"`.

> Обратные косые черты, которые не используются для экранирования кавычек, также должны быть экранированы другими обратными косыми чертами. Например: `${\"add_firewall_rule --ip_address=\" + ([.input.observables[] | select(.type == \"ip\") | select(.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.).*\") | not) | .value] | join(\",\"))}`.

Если вы хотите запустить плейбук для определенного объекта (наблюдаемые объекты или активы), используйте параметр `.input` в алгоритме. Эти объекты будут входными данными для плейбука при его запуске. Например:

```
"assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
```

Подробнее см. раздел Запуск плейбуков для объектов, указанных пользователями.

Как вызываются подсказки

Если вам нужна подсказка по доступным полям при написании алгоритма, используйте кавычки (`""`). Отобразится список доступных полей.

Чтобы отобразить подсказки по данным алерта или инцидента,

в jq-выражении напишите `alert` или `incident` и укажите точку `"."` в конце.

Правильная подсказка появляется, если в вышеуказанных выражениях нет ошибок. Иначе список доступных полей может быть некорректным.

Как вызываются подсказки

Вы можете вызывать подсказки при написании алгоритма плейбука. Подсказки содержат строку поиска и помогают вам быстро указать значение поля. Чтобы просмотреть подсказки, используйте кавычки (`""`). Отобразится список подсказок.

Подсказки также позволяют выполнять поиск по имени. Когда вы выбираете необходимое значение, имя автоматически изменяется на идентификатор в алгоритме. Подробнее см. Изменение инцидентов с использованием плейбуков и Изменение алертов с использованием плейбуков.

Если вы выберете и затем удалите имя параметра, указанное в кавычках, подсказка для параметра не отобразится, даже если вы указали новый параметр в кавычках.

Чтобы вернуться в режим подсказки для параметра, выполните одно из следующих действий:

- Удалите кавычки и добавьте открывающую двойную кавычку. Автоматически будет добавлена закрывающая двойная кавычка, и отобразится подсказка.
- Введите любой символ между кавычками, а затем нажмите на клавишу **`Backspace`**. Это вернет вас в режим подсказки.

Если вы удалите имя параметра посимвольно, вы не выйдете из режима подсказки, даже если полностью удалите имя параметра.

Пример алгоритма плейбука

```
{
  "actionsSpecVersion": "1",
  "dslSpecVersion": "1.1.0",
  "version": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "blockLDAPAccount"
          "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
        },
        "onError": "stop"
      }
    },
    {
      "loop": {
        "batchSize": 1,
        "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and .DestinationProcessName
!= \"\")][] | .DestinationProcessName] }",
        "mode": "parallel",
        "onError": "stop",
        "steps": [
```

```
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
                "params": {
                  "path": "${ .[0] }"
                }
              }
            }
          }
        ]
      }
    },
    {
      "action": {
        "function": {
          "type": "avScan",
          "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
          "params": {
            "scope": {
              "allowScanNetworkDrives": false,
              "area": "full"
            },
            "wait": false
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

Параметры плейбука

Идентификатор параметра	Описание
`name`	Название плейбука. Указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`description`	Описание плейбука. Указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`version`	Версия плейбука. Минимальная длина – 1. Этот параметр является обязательным.
`dslSpecVersion`	Версия схемы DSL. Минимальная длина – 1. Этот параметр является обязательным.
`actionSpecVersion`	Версия схемы действий по реагированию. Минимальная длина – 1. Этот параметр является обязательным.
`playbookRunTimeout`	Максимальное время выполнения плейбука, включая ожидание в очереди. Максимальное значение – 48 часов (`48h`). Вы можете настроить максимальное время выполнения в часах (ч) и/или минутах (мин), например: По умолчанию указано значение `24h`.
`inputType`	Тип входящего объекта. Возможные значения: `alert` или `incident`. Тип входящего объекта указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`input`	Выражение jq, которое можно использовать для преобразования или фильтрации входящих данных перед выполнением плейбука.
`output`	Выражение jq, которое можно использовать для изменения вывода плейбука перед выполнением.
`timeouts`	Определения тайм-аута.
`executionFlow`	Шаги выполнения плейбука. Этот параметр является обязательным.

Параметры шага выполнения

Массив элементов шага выполнения описывает логику плейбука. Шаги выполняются в порядке, описанном в плейбуке. Есть несколько типов шагов выполнения:

- Действие
- Loop
- Parallel
- Decision
- UpdateData

Параметры Action

Параметры `Action` вызывают функцию реагирования.

Идентификатор параметра	Описание
`function`	Объект, определяющий действие по реагированию. Дополнительную информацию см. в разделе Параметры ResponseFunction.
`filterProduct`	Этот параметр позволяет фильтровать компоненты для выполнения действия по реагированию. По запросу плагины компонентов фильтруются по разрешенным и ограниченным компонентам. Например, параметр можно указать следующим образом: `"filterProduct": { "allowed": ["Название_приложения"] }`
`output`	Этот параметр позволяет изменить значение, возвращаемое действием по реагированию, с помощью выражения jq и поместить его в данные плейбука (локальные или операционные).
`timeout`	Этот параметр позволяет установить тайм-аут для вызова функциональности реагирования. Вы можете указать имя политики тайм-аута, установленной в плейбуке, или установить значения тайм-аута вручную. Если значение не указано, то используется значение тайм-аута по умолчанию.

`manualApprove`	Этот параметр позволяет настроить подтверждение действия по реагированию вручную. Возможные значения:
	• Логическое значение:
	  • `true` – ручное подтверждение включено с параметрами по умолчанию.
	  • `false` – ручное подтверждение выключено.
	• Объект `ManualApprove`.

`onError`	Этот параметр определяет поведение при возникновении ошибки во время выполнения действия по реагированию. Возможные значения: • `stop` – определяет прерывание плейбука в случае ошибки при выполнении действия по реагированию. • `continue` – определяет, что выполнение плейбука будет продолжено, даже если одно из действий по реагированию завершится с ошибкой. В этом случае плейбук запускает следующее действие по реагированию, указанное в алгоритме. По умолчанию указано значение `stop`. Обратите внимание, что при возникновении системной ошибки выполнение плейбука завершается с ошибкой независимо от указанного значения параметра `onError`.

Политика времени ожидания

Политика времени ожидания шагов выполнения. Система автоматически определяет политику времени ожидания по умолчанию.

Политику времени ожидания по умолчанию можно изменить, используя имя политики по умолчанию. В этом случае новая политика будет автоматически применяться ко всем шагам выполнения.

Идентификатор параметра	Описание
`name`	Имя политики времени ожидания.
`scheduleToCloseTimeout`	Максимальное время выполнения, включая ожидание в очереди и повторные попытки. Параметр указывается в строковом формате Go. Если значение не указано или равно 0, используется значение из поля `playbookRunTimeout`.

Output

Параметр `output` генерирует операционные данные в конце шага, которые затем будут переданы на следующий шаг. Укажите параметр `output`, если вы хотите использовать результаты текущего шага плейбука на следующем шаге.

Чтобы избежать перегрузки системы, рекомендуется ограничивать данные, помещаемые в данные плейбука (локальные или операционные).

Идентификатор параметра	Описание
`action`	Этот параметр определяет, будут ли данные плейбука (локальные или операционные) перезаписываться или объединяться. Возможные значения: • `merge` – новые данные объединяются с текущими данными. • `overwrite` – текущие данные перезаписываются новыми данными.
`filter`	Этот параметр определяет выражение jq для обработки выходных данных.

Подтвердить вручную

Идентификатор параметра	Описание
`timeout`	Время ожидания подтверждения вручную в минутах. Минимальное значение – 10 минут (`10m`), максимальное – 180 минут (`180m`). По умолчанию это значение равно 60 минут (`60m`).
`emailNotifications`	Этот параметр позволяет настроить отправку уведомлений по электронной почте.

Параметры уведомлений по электронной почте

Идентификатор параметра	Описание
`enabled`	Флаг для включения уведомлений по электронной почте.
`delay`	Этот параметр определяет задержку перед отправкой уведомления по электронной почте. Значение указывается в минутах. Минимальное значение – 5 минут (`5m`), максимальное – 30 минут (`30m`). По умолчанию это значение равно 10 минут (`10m`).

Loop

Прежде чем указать параметр `Loop`, убедитесь, что параметр `aggregate` также указан в алгоритме плейбука.

Параметры `Loop` используются для разделения массива входящих данных по элементам и для выполнения различных действий с элементами.

Идентификатор параметра	Описание
`input`	Выражение jq для создания массива или ссылки на массив.
`aggregate`	Этот параметр позволяет настроить правила агрегирования с помощью выражения jq.
`output`	Настройка того, как применить выходные данные к текущим данным плейбука. Возможные значения: • Строковая константа: `merge` или `overwrite`. • Объект `Output`.
`mode`	Режим работы Loop. Возможные значения: • `parallel` – определяет, что все элементы обрабатываются параллельно. Количество потоков контролируется интерпретатором. • `sequence` – определяет, что все элементы обрабатываются последовательно. По умолчанию значение равно `parallel`.
`batchSize`	Этот параметр позволяет указать количество элементов массива, которые будут обрабатываться в одном цикле или в одном параллельном потоке. Вы можете использовать этот параметр, если функция плагина ограничивает количество входных элементов. Например, если функция плагина может обрабатывать не более 10 элементов в одном цикле, вы можете указать следующее значение параметра: `batchSize = 10`. По умолчанию значение равно `1`.

`onError`	Этот параметр определяет поведение при возникновении ошибки в одной из веток. Возможные значения:
	• `stop` – определяет завершение всех веток, если произошла ошибка. Остальные ветки продолжат работу.
	  • Если `mode=sequence`, после возникновения ошибки в одной ветке все последующие ветки будут остановлены.
	  • Если `mode = parallel`, после возникновения ошибки в одной ветке все ветки будут продолжать работать независимо друг от друга.
	• `continue` – определяет остановку одной из веток, в которой произошла ошибка. Остальные ветки продолжат работу.
	По умолчанию указано значение `stop`.

`steps`	Массив шагов запуска.

Parallel

> Прежде чем указать параметр `Parallel`, убедитесь, что параметр `aggregate` также указан в алгоритме плейбука.

Параметры `Parallel` используются для одновременного выполнения нескольких действий с данными. В отличие от Loop, параметр `Parallel` передает одни и те же входные данные в разные ветки выполнения.

Идентификатор параметра	Описание
`input`	Выражение jq для составления массива.
`aggregate`	Этот параметр позволяет настроить правила агрегирования с помощью выражения jq.
`output`	Настройка того, как применить выходные данные к текущим данным плейбука. Возможные значения: • Строковая константа: `merge` или `overwrite`. • Объект `Output`.
`onError`	Этот параметр определяет поведение при возникновении ошибки в одной из веток. Возможные значения: • `stop` – определяет завершение всех веток, если произошла ошибка. Остальные ветки продолжат работу. • `continue` – определяет остановку одной из веток, в которой произошла ошибка. Остальные ветки продолжат работу. По умолчанию указано значение `stop`.
`branches`	Ветки выполнения.

Ветка

Идентификатор параметра	Описание
`name`	Имя ветки, уникальное для `Parallel`.
`steps`	Массив шагов запуска.

Decision

Шаг `Решение` позволяет выполнить шаг или набор шагов в соответствии с условием. Обратите внимание, что выполняется только первое проверенное условие.

Идентификатор параметра	Описание
`conditions`	Массив условий.

Условие

Идентификатор параметра	Описание
`condition`	Выражение jq, содержащие условия выполнения.
`steps`	Шаги выполнения для текущей ветки.

UpdateData

Параметр *UpdateData* можно описать либо как jq-скрипт с логикой изменения состояния, либо как объект `Output`.

Параметры ResponseFunction

Идентификатор параметра	Описание
`action`	Название действия по реагированию.
`params`	Параметр позволяет описать параметры действия по реагированию, которое вы хотите запустить. Вы можете указать параметр как выражение jq или как объект. Параметры действий по реагированию описаны в таблице ниже.
`assets`	Параметр позволяет использовать выражение jq или массив строк, чтобы указать список активов, для которых вы хотите запустить действие по реагированию. Параметр `assets` необходим для действий по реагированию с активами и не применим для действий по реагированию без активов.

Параметры действий по реагированию

Название действия по реагированию	Параметры

`updateBases`	Действием по реагированию является обновление баз. Возможные параметры:
	• `wait`. Возможные значения:
	  • `true`
	  • `false`
	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`avScan`	Действием по реагированию является поиск вредоносного ПО. Возможные параметры:
	• `wait`. Возможные значения:
	  • `true`
	  • `false`
	• `scope`. Возможные значения:
	  • `full` – выполнить полную проверку устройства, на котором обнаружен алерт.
	  • `critical` – выполнить проверку памяти ядра, запущенных процессов и загрузочных секторов жесткого диска.
	  • `selective` – выполнить проверку указанных файлов. Чтобы указать путь к файлам, используйте параметр `path`.
	• `allowScanNetworkDrives`. Возможные значения:
	  • `true`
	  • `false`
	  По умолчанию значение равно `false`.
	  Этот параметр доступен, только если вы хотите выполнить полную проверку.
	  Обратите внимание, что проверка сетевых дисков может привести к перегрузке системы.
	• `path` – выражение jq или строка с путем к файлам, которые вы хотите проверить. Также вы можете указать несколько путей к файлам.
	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`moveHostsToAdministrationGroup`	Действием по реагированию является перемещение в группу. Возможные параметры: • `group` – путь к группе администрирования Open Single Management Platform. Например, `HQ/OrgUnit1`. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`quarantineFile`	Действием по реагированию является перемещение на карантин. Возможные параметры: • `path` – путь к файлу, который нужно поместить на карантин. • `md5` – MD5-хеш файла. • `sha256` – SHA256-хеш файла. Вы можете указать параметры действия по реагированию одним из следующих способов: • Укажите полный путь к файлу, который вы хотите поместить на карантин. В этом случае вам не нужно указывать хеш MD5 или хеш SHA256. • Укажите путь к файлу и хеш файла (MD5 или SHA256). Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`restoreQuarantinedFile`	Действие по реагированию "Восстановить файл из карантина". Возможные параметры: • `path` – путь к файлу, который вы хотите восстановить. • `md5` – MD5-хеш файла. • `sha256` – SHA256-хеш файла. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`killProcess`	Действием по реагированию является прерывание процесса. Возможные параметры: • `pid` – идентификатор процесса. • `path` – путь к файлу, который нужно поместить на карантин. • `md5` – MD5-хеш файла. • `sha256` – SHA256-хеш файла. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`changeAuthorizationStatus`	Действием по реагированию является изменение статуса авторизации. Возможный параметр:
	• `authorized`. Возможные значения:
	  • `true`
	  • `false`
	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`netIsolateOn`	Действием по реагированию является включение изоляции сети. Возможные параметры:
	• `isolationTimeoutSec` – период изоляции сети. Вы можете указать этот параметр в часах или днях.
	Минимальное значение в часах – 1 час, максимальное – 9999 часов.
	  Период изоляции сети указывается в секундах.
	• `exclusions` – правила исключения. Вы можете указать одно или несколько правил исключения.
	  • `remoteIPV4Address` – сетевой трафик с указанного IPv4-адреса будет исключен из блокировки. Например, `192.168.2.15`.
	  • `remoteIPV6Address` – сетевой трафик с указанного IPv6-адреса будет исключен из блокировки. Например, `2001:0db8:0000:0000:0000:ff00:0042`.
	  • `remotePortRange` – интервал удаленных портов.
	  • `localPortRange` – интервал локальных портов.
	  Если `remotePortRange` и `localPortRange` не указаны, правило исключения применяется ко всем портам.
	• `exclusionsConflictBehavior` – определяет поведение в случае конфликта между различными правилами исключения. Возможные параметры:
	  • `replace`
	  • `skip`
	  • `fail`

`netIsolateOff`	Действием по реагированию является выключение изоляции сети. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`executeCommand`	Действием по реагированию является запуск исполняемого файла. Возможные параметры: • `commandLine` – команда для запуска или полный путь к исполняемому файлу. • `workingDirectory` – путь к рабочей директории. • `commandLineParameters` – параметры командной строки, которые вы хотите применить к команде. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`addFilePreventionRules`	Действием по реагированию является добавление правила запрета. Возможные параметры: • `md5` – хеш-массив MD5. • `sha256` – хеш-массив SHA256. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`deleteFilePreventionRules`	Действием по реагированию является удаление правила запрета. Возможные параметры: • `md5` – хеш-массив MD5. • `sha256` – хеш-массив SHA256. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`resetFilePreventionRules`	Действием по реагированию является удаление всех правил запрета. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`assignKasapGroup`	Действием по реагированию является назначение KASAP-группы. Возможные параметры: `groupId` – идентификатор группы KASAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`addToLDAPGroup`	Действием по реагированию является добавление пользователя в группу безопасности. Возможные параметры: `groupDN` – отличительное имя (DN) группы LDAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`removeFromLDAPGroup`	Действием по реагированию является удаление пользователя из группы безопасности. Возможные параметры: `groupDN` – отличительное имя (DN) группы LDAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`blockLDAPAccount`	Действием по реагированию является блокировка учетной записи. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`resetLDAPPassword`	Действием по реагированию является сброс пароля. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`executeCustomScript`	Действием по реагированию является выполнение пользовательских скриптов. Возможные параметры: • `commandLine` – команда для запуска. • `commandLineParameters` – параметры командной строки, которые вы хотите применить к команде. • `stdIn` – стандартный входной поток. Используйте этот параметр, если для выполнения скрипта требуются дополнительные данные из стандартного ввода. • `workingDirectory` – путь к рабочей директории.

`iocsEnrichment`	Действием по реагированию является обогащение данных. Возможные параметры:
	• `observables` – выражение jq с массивом наблюдаемых объектов, которые вы хотите обогатить.
	• `fullEnrichment` – определяет количество запрошенных записей. Возможные значения:
	  • `true` – запрашивать все записи из источника.
	  • `false` – запрашивать 100 самых популярных записей из источника.

AI-сервисы

В этом разделе представлена информация об AI-сервисах, с которыми работает Kaspersky EDR Expert.

AI рейтинг и AI-статус активов

Сервис **AI-оценка и AI-статус активов** доступен для установки, если лицензия содержит модуль AI.

AI-сервис позволяет уточнить критичность корреляционных событий, сгенерированных в результате срабатывания правил корреляции.

AI-сервис получает из доступных кластеров хранения корреляционные события, содержащие непустое поле **Affected assets**, выстраивает ожидаемую последовательность событий и обучает модель AI. На основании цепочки срабатываний корреляционных правил AI-сервис высчитывает, является ли такая последовательность срабатываний характерной в этой инфраструктуре. Нехарактерные паттерны повышают рейтинг актива.

По результатам расчетов AI-сервиса в карточке активов становится доступным для просмотра **AI-рейтинг** и **AI-статус**. Если лицензионный ключ удалить, поля **AI-рейтинг** и **AI-статус** будут скрыты из карточки актива. Если лицензионный ключ снова добавить, значения полей **AI-рейтинг** и **AI-статус** снова будут отображаться.

Рейтинг – это число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля **AI-статус**: **Low**, **Medium**, **High**, **Critical**. Значение рейтинга может быть от 0 до 1.

Существует 4 диапазона, по которым присваивается значение статуса:

0 <= рейтинг < 0.25 - Low

0.25 <= рейтинг < 0.5 - Medium

0.5 <= рейтинг < 0.75 - High

0.75 <= рейтинг <= 1 - Critical

Вы можете осуществлять поиск активов с помощью фильтра по полям **AI-рейтинг** и **AI-статус**. Также вы можете настроить проактивную категоризацию активов по полям **AI-рейтинг** и **AI-статус** и тогда, как только AI-сервис присвоит активу рейтинг, актив будет перемещен в заданную для такого уровня риска категорию.

Вы можете создать структуру из нескольких категорий и автоматически наполнять их активами в соответствии с вычисленными значениями риска.

В разделе **Параметры** → **Аудит активов** вы можете настроить создание событий аудита при добавлении актива в категорию. События аудита могут учитываться в правилах корреляции, а также их можно отслеживать на панели мониторинга и в отчетах.

Чтобы отслеживать изменение категории активов на панели мониторинга, создайте виджет **События** с запросом следующего вида:

```
SELECT count(ID) AS `metric`,
formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value` FROM `events`

where DeviceVendor = 'Kaspersky' and DeviceProduct = 'KUMA' and

DeviceEventCategory = 'Audit assets' and DeviceAction= 'asset added to category'

and DeviceCustomString1 = 'Main/Categorized assets/ML/score>0.5'

GROUP BY Timestamp ORDER BY value LIMIT 250
```

Чтобы отслеживать распределение активов по статусам на панели мониторинга, создайте виджет **Активы по уровню важности**. Виджет **Активы по уровню важности** доступен, если лицензия содержит модуль AI. На круговом графике будет отображаться количество активов с группировкой по статусу.

После каждого перезапуска AI-сервиса, AI-сервис заново обучает модель и выполняет переоценку рейтинга активов, указанных в событиях за сегодня.

В директории, указанной в конфигурационном файле, хранятся события, которые AI-сервис получил из кластеров хранения KUMA за указанное количество дней. Например, если в конфигурационном файле указано 12 дней, AI-сервис будет получать события за последние 12 дней. Самые давние события удаляются из директории. В этой же директории будет храниться обученная модель.

Переобучение модели происходит в полночь по UTC. Переоценка рейтинга активов происходит раз в час для всех активов, которые были в событиях за сегодня по UTC.

Журналы сервиса хранятся в /var/log/syslog.

Установка сервиса AI-рейтинг и AI-статус активов

Установка сервиса AI-рейтинг и AI-статус активов

Чтобы установить сервис:

1. Распакуйте архив **mlservice-installer-XX.tgz**, который входит в поставку.

   Архив **mlservice-installer-XX.tgz** содержит скрипты для установки и удаления сервиса, а также конфигурационный файл config.yaml.

2. В конфигурационном файле config.yaml в параметре `kuma_address` укажите FQDN хоста, на котором установлено Ядро KUMA, и порт, по которому Ядро KUMA будет ожидать подключения AI-сервиса.

   В установке в отказоустойчивой конфигурации должен быть указан порт 7226. Для остальных параметров можно оставить значения по умолчанию. После установки сервис запустится с использованием параметров, заданных в файле config.yaml.

3. Если вы хотите установить сервис на удаленный хост, укажите в inventory.yaml адрес удаленного хоста и убедитесь в наличии сетевого доступа. По умолчанию сервис устанавливается на локальный хост, как указано в inventory.yaml.

4. Получите сертификат Ядра в веб-интерфейсе KUMA. Для этого в главном окне веб-интерфейса KUMA нажмите на имя своей учетной записи внизу окна и в открывшемся меню выберите пункт **Сертификат AI-сервиса**. Сертификат будет скачан в директорию загрузок по умолчанию.

   При необходимости вы можете перевыпустить сертификат AI-сервиса.

5. Переименуйте скачанный файл сертификата в **core-external-ca.cert**.

6. Сохраните файл сертификата Ядра KUMA в директории установщика roles/mlservice/files.

7. Перейдите в директорию с файлами сервиса и из этой директории выполните команду:

   ```
   ./install < путь к inventory.yaml >
   ```

8. Если вы готовы принять условия Лицензионного соглашения, нажмите Y. Если вы не примете условия Лицензионного соглашения, вы не сможете продолжить установку сервиса. Файл с текстом Лицензионного соглашения доступен в директории mlservice-installer\eula.

9. Установщик генерирует необходимые сертификат и ключ в процессе установки и помещает их в директории, указанные в конфигурационном файле config.yaml. Сертификат необходимо загрузить в KUMA.

   В веб-интерфейсе KUMA в разделе **Параметры** → **Интеграции** → **AI-сервисы** в окне **AI-оценка и AI-статус активов** заполните следующие поля:

   a. В поле **URL** укажите FQDN хоста, на котором установлено Ядро KUMA, и порт, по которому Ядро KUMA будет ожидать подключения AI-сервиса, например: <FQDN хоста, на котором установлено Ядро KUMA>:7226. Номер порта должен соответствовать указанному в конфигурационном файле. Убедитесь, что порт не занят другими приложениями.

      Для установки KUMA в отказоустойчивой конфигурации поле **URL** не отображается в интерфейсе, значение порта берется из переменной окружения KUMA_APPRAISER_AI_API_PORT и порт открывается для всех IP-адресов хоста Ядра KUMA.

   b. В поле **Сертификат** в раскрывающемся списке выберите **Создать**, в открывшемся окне **Создание секрета** укажите тип секрета **Certificate** и загрузите сертификат из директории, указанной в конфигурационном файле config.yaml.

   c. Включите переключатель **Состояние**. По умолчанию переключатель выключен.

   d. Нажмите **Сохранить**.

   Сразу после установки сервис будет пытаться в течение 15 минут подключиться к KUMA с интервалом в 1 минуту. Если сертификат не добавлен в веб-интерфейсе KUMA, подключение не будет выполнено и сервис остановится. В таком случае можно добавить сертификат и перезапустить AI-сервис, сервис попробует подключиться повторно.

   После сохранения параметров получите журнал сервера Ядра и убедитесь в отсутствии ошибки <номер порта>: bind: address already in use.

AI-сервис установлен.

Удаление сервиса AI-рейтинг и AI-статус активов

Чтобы удалить AI-сервис, перейдите в директорию с файлами AI-сервиса и из этой директории выполните команду:

```
./uninstall <путь к inventory.yaml>
```

Перевыпуск сертификата AI-сервиса

Чтобы перевыпустить сертификат AI-сервиса:

1. В Консоли OSMP перейдите в раздел **Параметры** → **Другое** → **Общее.**
2. В блоке **Параметры Ядра** для параметра **Сертификат AI-сервиса** нажмите на кнопку **Перевыпустить.**
3. Для подтверждения операции нажмите **OK**.
4. Замените сертификат в директории /opt/kaspersky/mlservice/ на новый сертификат.
5. Перезапустите сервис AI-рейтинга и AI-статуса активов, выполнив команду `systemctl restart mlservice`, и Ядро KUMA.

Новый сертификат AI-сервиса будет применен.

Параметры настройки сервиса AI-рейтинг и AI-статус активов

Доступные параметры настройки AI-сервиса

Параметр	Описание
`cert_file_path`	Путь к директории, где лежит сгенерированный установщиком сертификат. Путь по умолчанию: /opt/kaspersky/mlservice/service.crt Вы можете указать другой путь. В таком случае следует убедиться, что у пользователя, под которым запускается сервис, есть доступ к указанной директории.
`key_file_path`	Путь к директории, где лежит сгенерированный установщиком ключ. Путь по умолчанию: /opt/kaspersky/mlservice/service.key Вы можете указать другой путь. В таком случае следует убедиться, что у пользователя, под которым запускается сервис, есть доступ к указанной директории.
`kuma_address`	FQDN хоста, на котором установлено Ядро KUMA и порт, по которому Ядро KUMA будет ожидать подключения AI-сервиса. Для установки в отказоустойчивой конфигурации следует указать порт 7226. Пример: <FQDN хоста, на котором установлено Ядро KUMA>:7226
`kuma_cert_file_path`	Путь к директории, где размещается сертификат Ядра KUMA. Путь по умолчанию: /opt/kaspersky/mlservice/core-external-ca.cert

Параметр	Описание
`event_storage_path`	Путь к директории, где сервис разместит полученные корреляционные события. Путь по умолчанию: /var/mlservice/events
`model_storage_path`	Путь к директории, где сервис разместит обученную модель. Путь по умолчанию: /var/mlservice/models
`period_for_train_days`	Количество дней, за которые нужно получить из доступных кластеров хранения корреляционные события, в которых фигурируют активы, для обучения модели. Значение по умолчанию: 12 дней. Это означает, что в директории всегда будут события за последние <N> дней. Самые давние события удаляются.
`events_overlap_in_seconds`	Время перекрытия. Когда события для оценки рейтинга активов скачиваются по расписанию, они берутся от времени последнего скачанного события за сегодня минус значение параметра events_overlap_in_seconds. Значение по умолчанию: 60 секунд. Пример: время получения последнего события – 8:58. Следующая партия событий будет скачиваться начиная с 8:57.

Настройка интеграции с KIRA с использованием поставщика LLM

KIRA поддерживает работу со следующими сторонними LLM-провайдерами:

- GPT-5.4
- Deepseek-V4-Pro
- Kimi K2.6
- GLM-5.1
- MiniMax M2.7

Чтобы настроить интеграцию с KIRA с использованием стороннего LLM-провайдера:

1. Получите лицензию с AI-модулем и активируйте функциональность в KUMA.
2. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.
   Откроется окно с параметрами KUMA.
3. В разделе **Интеграции** нажмите **AI-сервисы**.
4. В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant**.
5. Включите интеграцию с KIRA, установив переключатель **Статус** в активное положение.
   По умолчанию переключатель выключен.
6. В блоке параметров **Режим** выберите режим работы с KIRA **Custom**. По умолчанию выбран режим **KSN**.

7. В поле **Базовый URL** укажите API-адрес провайдера (например: https://api.openai.com/v1). Адрес должен начинаться с http:// или https://.

8. В раскрывающемся списке **API ключ** выберите секрет типа **token** или создайте новый.

   Для создания нового секрета выберите значение **Создать**. Если используемый API не требует ключа, в поле **API ключ** укажите секрет со значением **api-key**.

9. В поле **Модель** укажите имя модели, используемой провайдером (например: gpt-4-turbo, llama3-70b).

10. В поле **Максимальный размер промпта** укажите максимальное количество токенов в запросе.

11. В раскрывающемся списке **Прокси-сервер** выберите ранее созданный ресурс или создайте новый.

12. Выберите язык ответа на запрос в KIRA: русский или английский. KUMA будет передавать и хранить ответы KIRA на выбранном вами языке.

    По умолчанию выбран русский язык.

13. Нажмите на кнопку **Добавить файл JSON**, чтобы загрузить файл с заданными параметрами модели и HTTP-заголовками.

    Вы можете указать в файле дополнительные параметры запроса к LLM-провайдеру (например `temperature`, `max_tokens`). Также вы можете задать дополнительные HTTP-заголовки. Для этого нужно использовать ключ `"headers"`. Если в файле указано несколько ключей `"headers"`, используется только первый из них.

    Пример содержания файла

    ```
    {
      "temperature": 0.5,
      "max_tokens": 20000,
      "headers": {
        "OpenAI-Organization": "ORG_ID"
      }
    }
    ```

    Если в JSON-файле указан хотя бы один из следующих параметров, AI-сервис вернет ошибку: `messages`, `model`, `audio`, `function_call`, `functions`, `modalities`, `n`, `parallel_tool_calls`, `prediction`, `response_format`, `stop`, `stream`, `stream_options`, `tool_choice`, `tools`, `web_search_options`.

14. Нажмите **Проверить подключение**, чтобы выполнить тестовый запрос к указанному API.

15. Нажмите **Сохранить**.

    После того как вы нажмете **Сохранить**, вам будет предложено принять условия Лицензионного соглашения. Если вы не примете соглашение, сохранить параметры и продолжить работу с функциональностью будет невозможно.

    После сохранения параметров будет показано доступное количество токенов. Количество токенов обновляется ежедневно.

Интеграция будет настроена, можно переходить к анализу. Анализ доступен для всех событий, новых и уже полученных.

Анализ алертов и инцидентов с помощью KIRA

Режим Kaspersky Security Network (KSN) для Kaspersky Investigation and Response Assistant доступен только в регионе RU.

Вы можете использовать Kaspersky Investigation & Response Assistant (KIRA) для анализа алертов и инцидентов. По итогам анализа вы получаете автоматически созданное описание алерта или инцидента, которое включает в себя краткую сводку, список наблюдаемых объектов, временную шкалу событий, отчет по алерту или инциденту и рекомендации по устранению уязвимостей.

Эта функция может ускорить расследование и первоначальный анализ алертов или инцидентов безопасности. Она доступна вне зависимости от того, какие типы событий связаны с алертом или инцидентом.

В зависимости от настроенного режима KIRA:

- При использовании Kaspersky Security Network (режим **KSN**) запрос отправляется через облачную службу "Лаборатории Касперского".
- При использовании стороннего поставщика LLM (**Пользовательский** режим) запрос отправляется непосредственно в указанный API.

  Пользователь выбирает поставщика, модель и параметры. Обработка данных выполняется на стороне выбранной службы.

Функция доступна при выполнении следующих условий:

- Наличие действующей лицензии с модулем AI.

  Если срок лицензии истек, результаты анализа будут доступны через задачи в течение срока жизни кеша, то есть в течение 14 дней с момента попадания результатов в кеш.
- Для интеграции с KIRA с использованием KSN предоставлен сертификат.
- Для интеграции с KIRA с использованием стороннего поставщика LLM было настроено подключение к API поставщика.
- Пользователь имеет права на **Запись** в функциональную область **Алерты и инциденты**.

Настройка интеграции с KIRA с использованием KSN

Для интеграции с KIRA вам потребуется сертификат. Файл сертификата в формате PFX, запакованный в архив <имя заказчика>.ZIP, и пароль к сертификату, можно получить у сотрудников Службы технической поддержки.

Чтобы настроить интеграцию с KIRA с использованием KSN:

1. Получите лицензию с AI-модулем и активируйте функциональность в KUMA.
2. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

3. В разделе **Интеграции** нажмите **AI-сервисы**.

4. В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant**.

5. Включите интеграцию с KIRA, установив переключатель **Статус** в активное положение.

   По умолчанию переключатель выключен.

6. В блоке параметров **Режим** выберите режим KIRA **KSN**.

7. Нажмите **Выбрать файл** и загрузите архив <название организации>.ZIP, в котором содержится сертификат в формате PFX.

8. В поле **Пароль от сертификата** укажите пароль.

9. В раскрывающемся списке **Прокси** выберите ранее созданный ресурс или создайте новый.

10. В раскрывающемся списке выберите язык ответа на запрос в KIRA, русский или английский. KUMA будет передавать и хранить ответы KIRA на выбранном языке.

    По умолчанию выбран русский язык.

11. Нажмите на кнопку **Сохранить**.

    После того как вы нажмете **Сохранить**, вам будет предложено принять условия Лицензионного соглашения. Если вы не примете Лицензионное соглашение, сохранить параметры и продолжить работу с функциональностью будет невозможно.

    После сохранения параметров отобразится доступное количество токенов. Количество токенов обновляется ежедневно.

Интеграция будет настроена, можно переходить к анализу алертов и инцидентов.

Выполнение анализа с помощью KIRA

После того как интеграция настроена, можно выполнять анализ алертов и инцидентов с помощью KIRA.

Чтобы выполнить анализ:

1. Откройте детали алерта или инцидента.

2. На панели инструментов в верхней части раздела деталей алерта или инцидента нажмите **AI-анализ** → **Проанализировать с помощью KIRA**.

   Если достаточно токенов, запустится выполнение анализа и задача **Запрос в KIRA**.

   Выполнение запроса может занимать от 30 секунд и дольше.

   Расход токенов осуществляется, даже если получен ответ с ошибкой о том, что запрашиваемая тема находится в запрещенном списке, при этом сведения о доступном остатке токенов тоже будут обновлены.

Анализ алерта или инцидента будет выполнен.

Чтобы просмотреть результаты анализа, на панели инструментов в верхней части раздела деталей алерта или инцидента нажмите **AI-анализ** → **Просмотр отчета**. В окне **Проанализировать с помощью KIRA** отображается результат анализа, который включает в себя следующую информацию:

- краткое описание алерта или инцидента;
- список наблюдаемых объектов;
- хронологию событий, связанных с алертом или инцидентом, с временной шкалой;
- отчет о происшествии;
- дату и время последнего запроса;
- количество израсходованных токенов.

Вы можете нажать на кнопку **Повторный анализ**, чтобы выполнить новый анализ без учета данных предыдущего, хранящихся в кеше. При проведении этого анализа будут израсходованы токены.

Возможные ошибки задачи Проанализировать с помощью KIRA

При проведении анализа алертов и инцидентов с помощью KIRA могут возникать ошибки.

Возможные ошибки

HTTP-код	Описание
400	Неверный запрос к службе или недействительный клиентский сертификат. Возможные причины: необходимые параметры отсутствуют или содержат недопустимые значения; срок действия клиентского сертификата, используемый для KSN, истек, или сертификат выдан ненадежным центром сертификации.
401	Не удалось выполнить аутентификацию. Клиентский сертификат действителен, но в базе данных лимитов нет соответствующей ему записи. Возможные причины: запись была удалена или не была своевременно создана, либо из-за технической ошибки были записаны неверные данные.
403	Ежедневное ограничение по токенам превышено.
404	Неизвестная или не поддерживаемая пользовательская задача
413	Превышен лимит токенов для запроса. Запрос содержит слишком много входных токенов. Максимально допустимое количество токенов на один запрос – 16 000, включая параметры службы. Если этот предел превышен, анализ не будет проведен.
500	Внутренняя ошибка службы. При обработке запроса произошла неизвестная ошибка.
502	AI-сервис недоступен. KIRA недоступен.
503	Ошибка подключения службы. Не удалось получить токен доступа от KIRA.
Другое	Ошибка подключения. Любой другой код ошибки, не указанный выше, который возвращает службу KSN.
Без кода	Ошибка при обработке запроса на стороне KUMA. Возможные причины включают ошибку при чтении ответа от KSN, ошибку при сохранении данных в базе данных или ошибку при получении параметров интеграции.

Создание поисковых запросов на естественном языке с помощью KIRA

В разделе **Поиск угроз** доступна возможность ввести поисковый запрос на естественном языке, автоматически преобразовать запрос с помощью Kaspersky Investigation & Response Assistant (далее KIRA) в синтаксис поискового запроса к базе событий, проверить корректность и уточнить запрос при необходимости, а затем запустить сформированный системой запрос и получить результаты поиска по событиям. Каждый раз при отправке запроса создается событие аудита. В случае ошибки при генерации запроса отображается код ошибки.

Ограничение токенов общее для следующих действий:

- Построение поисковых запросов на естественном языке с помощью KIRA.
- Проанализировать с помощью KIRA.

Итоговое количество токенов зависит от запроса и ответа. Вы можете предварительно посмотреть количество токенов, которые будут потрачены на отправку запроса и получение ответа, и изменить запрос, чтобы потратить меньше токенов.

Функция доступна в регионе RU при следующих условиях:

- Наличие действующей лицензии с модулем AI.
- При настройке интеграции с KIRA загружен сертификат. Файл сертификата в формате PFX, запакованный в архив <название компании>.ZIP, и пароль к сертификату, можно получить у сотрудников Службы технической поддержки.
- Пользователю назначена одна из ролей с правами доступа: Главный администратор, Администратор, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик. Настройка интеграции доступна только пользователю с ролью Главный администратор.

Создание поисковых запросов на естественном языке и их преобразование в SQL-запросы с помощью KIRA

После того как интеграция с KIRA настроена, можно построить поисковый запрос к событиям.

Чтобы построить поисковый запрос на естественном языке и преобразовать в SQL-запрос с помощью KIRA:

1. В разделе **Поиск угроз** под полем для ввода SQL-запроса нажмите на кнопку ( ).
2. В открывшемся окне в поле для ввода запроса введите текст запроса, который необходимо преобразовать в формат SQL с помощью KIRA.

   Например: "Покажи все события с 15 по 16 января 2024 года, где имя файла было "file.txt"".

   Поддерживается преобразование запросов, составленных на русском и английском языках.
3. Нажмите на кнопку **Сгенерировать**.

   В поле для вывода отображается сгенерированный SQL-запрос.

Например:

```
SELECT *
FROM events
WHERE FileName = 'file.txt'
ORDER BY Timestamp DESC
```

В поле **Период** отображается сгенерированный временной интервал:

Например:

2024-01-15T00:00:00.000 - 2024-01-16T00:00:00.000

Если в своем тексте вы не указали временной диапазон, в рамках которого необходимо выполнить поиск событий, устанавливается тот диапазон, который был указан на вкладке **События**. Например, если в разделе **События** было установлено значение 5 мин, и запрос был отправлен в 15 января в 15:30, подставится значение 2026-01-15T15:25:00.000 - 2026-01-15T15:30:00.000

Вы можете изменить значения в полях **SQL-запрос** и **Период** до применения сгенерированного запроса.

4. Если вы хотите узнать, сколько токенов будет потрачено на генерацию запроса, нажмите **Рассчитать требуемое число в токенах**.

5. Если вы хотите использовать сгенерированный SQL-запрос для поиска по событиям, нажмите на кнопку **Применить**.

   Окно **Сгенерировать SQL-запрос с помощью KIRA** автоматически закрывается.

   Сгенерированный SQL-запрос автоматически подставляется в основное поле запросов на вкладке **Поиск угроз**.

   Поле абсолютного диапазона времени автоматически заполняется значениями из сгенерированного запроса.

   Например: 2026-01-15T00:00:00.000 - 2026-01-15T00:00:00.000

6. Если вы хотите выполнить поиск по событиям с использованием сгенерированного SQL-запроса, нажмите **Выполнить запрос**.

Поисковый запрос на естественном языке преобразован в SQL-запрос и получен результат поиска по событиям.

Возможные ошибки при создании запроса на естественном языке

Возможные ошибки

HTTP-код	Описание
400	Недействительный клиентский сертификат.
404	Ошибка в запросе.
401	Отсутствует информация о сертификате. Обратитесь в Службу технической поддержки.
403	Суточный лимит токенов исчерпан.
413	Достигнуто максимальное количество токенов для выполнения запроса. Следует уменьшить запрос.
422	Из запроса невозможно сформировать SQL-запрос.

HTTP-код	Описание
500	Неизвестная ошибка сервиса.
502	Сервис KIRA недоступен.
503	Ошибка получения токена доступа в сервисе.
Другое	Неизвестная ошибка.
Без кода	Ошибка при обработке запроса.

Настройка обнаружения атак DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легальное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Уязвимое программное обеспечение при запуске не проверяет легитимность динамической библиотеки и загружает ее по имени файла. В результате происходит исполнение вредоносного кода в контексте легального программного обеспечения. Атаку с использованием техники DLL Hijacking сложно обнаружить, так как фактически запускается легальное программное обеспечение. Для обнаружения таких атак использует модуль AI. Модуль AI анализирует параметры запуска и исполнения приложений и определяет подозрительные случаи запуска легального программного обеспечения с вредоносными библиотеками.

Для получения заключения KUMA отправляет запрос в KSN. Запрос содержит информацию из полей события, которая необходима для анализа. В ответ на запрос KSN присылает один из следующих результатов анализа:

- `0` – **В обработке**. Для получения заключения требуется отправить запрос повторно. Отправку повторных запросов вы можете настроить с помощью параметра **Выполнять повторный запрос**.
- `1` – **Вредоносность не подтверждена**. На момент получения заключения библиотека не считается вредоносной.
- `2` – **Подозрительная**. При получении такого результата создается алерт, если у вас настроено соответствующее правило корреляции.
- `3` – **Вредоносная**. При получении такого результата создается алерт, если у вас настроено соответствующее правило корреляции. Заключение **Вредоносная** с большей вероятностью указывает на обнаружение DLL Hijacking, чем заключение **Подозрительная**.

Заключение записывается в событие в поле KL_AI_DLLHijackingCheckResult в виде числового значения и текстового пояснения.

Обнаружение атак DLL Hijacking производится на этапе обогащения событий. Для этого используется обогащение типа **проверка DLL Hijacking**. Обогащение этого типа вы можете встроить либо в коллектор, либо в коррелятор. Рекомендуется встраивать обогащение этого типа в коррелятор. В этом случае нагрузка на службу KSN значительно ниже, чем при проверке событий в коллекторе.

Для использования обогащения типа **проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главный администратор также должен принять дополнительное Положение о KSN в разделе **Kaspersky Security Network** (**Параметры** → **Интеграции** → **AI-сервисы** → **Kaspersky Security Network**). Если в вашем экземпляре KUMA несколько главных администраторов, достаточно, чтобы Положение принял любой из них.

Обнаружение атак DLL Hijacking с помощью обогащения событий в корреляторе

Чтобы настроить обнаружение атак DLL Hijacking с помощью обогащения событий в корреляторе:

1. В веб-интерфейсе приложения перейдите в раздел **Ресурсы** → **Корреляторы**.

2. Запустите создание коррелятора или откройте параметры существующего коррелятора.

3. Добавьте обогащение типа Проверка DLL Hijacking.

   При настройке обогащения вам нужно указать список полей, которые соответствуют параметрам, необходимым для создания запроса в KSN. Убедитесь, что указанные вами поля заполняются при нормализации в коллекторе.

4. В параметрах обогащения в разделе **Параметры фильтра** выберите из списка фильтр **[OOTB] Events for DLLHijacking enrichment**. Filter for correlator. Если этот фильтр отсутствует в списке, импортируйте его из репозитория. Вы также можете настроить фильтр самостоятельно.

5. Если вы хотите настроить приложение так, чтобы при получении заключений **Подозрительная** или **Вредоносная** создавался алерт, создайте соответствующее правило корреляции. При создании правила корреляции выберите тип simple или тип standard и на вкладке **Селектор** укажите в параметрах фильтра два условия:

   `KL_AI_DLLHijackingCheckResult = 2` или `KL_AI_DLLHijackingCheckResult = 3`

   Также в правиле корреляции укажите поля, которые вы указали при добавлении обогащения (см. п.3 инструкции). Поля должны быть перечислены в параметре **Наследуемые поля**, если вы создали правило корреляции типа simple, или в параметре **Группирующие поля**, если вы создали правило корреляции типа standard.

Обнаружение атак DLL Hijacking с помощью обогащения событий в коллекторе

> Не рекомендуется использовать обогащение типа **Проверка DLL Hijacking** в коллекторе. Это повышает нагрузку на службу KSN. Вместо этого добавьте обогащение этого типа в коррелятор.

Чтобы настроить обнаружение атак DLL Hijacking с помощью обогащения событий в коллекторе:

1. В веб-интерфейсе приложения перейдите в раздел **Ресурсы** → **Коллекторы**.

2. Запустите создание коллектора или откройте параметры существующего коллектора.

3. Добавьте обогащение типа Проверка DLL Hijacking.

   При настройке обогащения вам нужно указать список полей, которые соответствуют параметрам, необходимым для создания запроса в KSN. Убедитесь, что указанные вами поля заполняются при нормализации в коллекторе.

4. В параметрах обогащения в разделе **Параметры фильтра** выберите из списка фильтр **[OOTB] Events for DLLHijacking enrichment**. Filter for collector. Если этот фильтр отсутствует в списке, импортируйте его из репозитория. Вы также можете настроить фильтр самостоятельно.

5. Если вы хотите настроить приложение так, чтобы при получении заключений **Подозрительная** или **Вредоносная** создавался алерт, создайте соответствующее правило корреляции. При создании правила корреляции выберите тип simple или тип standard и на вкладке **Селектор** укажите в параметрах фильтра два условия:

   `KL_AI_DLLHijackingCheckResult = 2` или `KL_AI_DLLHijackingCheckResult = 3`

   Также в правиле корреляции укажите поля, которые вы указали при добавлении обогащения (см. п.3 инструкции) и поле KL_AI_DLLHijackingCheckResult. Поля должны быть перечислены в параметре **Наследуемые поля**, если вы создали правило корреляции типа simple, или в параметре **Группирующие поля**, если вы создали правило корреляции типа standard.

Настройка обнаружения взломанных учетных записей

Для обнаружения атак, связанных с использованием скомпрометированной учетной записи, используется правило корреляции типа periodical. Это правило работает со статистическими данными: алгоритмы машинного обучения создают профиль нормального поведения пользователей и выявляют отклонения от этого поведения на основе статистических показателей. Процесс выявления аномалий выполняется с определенной периодичностью, указанной в файле `correlation-rules.yaml`, на основе накопленных данных, а не в момент поступления каждого события.

Вы можете создать корреляционное правило типа **periodical** только с помощью коррелятора correlator-ng.

Работа правила корреляции типа **periodical** состоит из двух этапов:

1. **Накопление и агрегация данных**

   На первом этапе правило корреляции накапливает статистику поведения пользователей. Этот этап соответствует периоду холодного старта, в течение которого аномалии не выявляются. Накопление статистики начинается с первого события, поступившего в правило. При этом все события, созданные ранее, не учитываются.

   В рамках этапа накопления и агрегации данных происходит следующее:

   - Принимаются события успешных и неуспешных попыток входа в учетную запись пользователя.
   - Извлекаются адреса, с которых и на которые проводился вход в систему.
   - Данные агрегируются по пользователям: сохраняются уникальные значения, формируются значения количества новых адресов для каждого периода группировки событий аутентификации.

   Продолжительность периода холодного старта фиксирована – она указана в параметрах правила корреляции. Холодный старт может быть выполнен следующими способами:

   - С помощью обработки потока событий, поступающего в коррелятор.
   - С использованием процедуры ретроспективного сканирования для загрузки событий из хранилища.
   - С помощью комбинированного метода, в рамках которого часть данных загружается с помощью ретроскана, а оставшиеся собираются за счет обработки потока событий.

   При использовании ретроспективного сканирования правило корреляции обрабатывает загружаемые события так же, как и события, поступающие из потока. Как только события аутентификации пользователей в хранилище начинают покрывать минимальный период времени, необходимый для сбора статистики, правило начинает периодически обнаруживать аномалии сразу после загрузки событий.

Допускается ситуация, при которой в правило сначала загружаются данные за период, не превышающий длительность холодного старта, а затем накопление статистики продолжается при обработке потока событий до завершения периода холодного старта.

2. **Обнаружение аномалий**

   После завершения периода холодного старта правило начинает анализировать накопленные данные с определенной периодичностью. Для каждого пользователя и каждого анализируемого признака:

   - Используется значение показателя за период группировки событий аутентификации.

     Если периоды обнаружения аномалии и группирования совпадают, для анализа используется значение показателя за последний завершенный период. Если период обнаружения короче периода группирования, анализ выполняется на основе данных, собранных за текущий период, благодаря чему можно получить результаты до завершения периода группирования.

   - Вычисляются статистические показатели.

   - Результаты сравниваются с пороговыми значениями, заданными в параметрах правила корреляции.

   Если показатели, отражающие аномальную активность пользователя, превышают пороговые значения, создается корреляционное событие. При необходимости правило может дополнительно создавать алерт.

Показатели выявления аномальной активности пользователей

Для выявления аномалий используются два показателя:

- **Relative Score (Относительный показатель)**

  Этот показатель показывает, во сколько раз текущая активность пользователя превышает его средний уровень активности, и рассчитывается по следующей формуле:

  Relative Score = (**Текущая активность** + 1) / (**Средняя активность** + 1)

  Здесь:

  Текущая активность – значение активности на текущий момент.

  Средняя активность – средний уровень активности за период, на основе которого рассчитывается показатель.

- **Z-Score (Стандартизированное отклонение)**

  Этот показатель показывает, насколько текущее значение отклоняется от среднего значения с учетом разброса данных, и рассчитывается по следующей формуле:

  Z-Score = (**Текущая активность** – **Средняя активность**) / **Стандартное отклонение**

  Здесь:

  Текущая активность – значение активности на текущий момент.

  Средняя активность – средний уровень активности за период, на основе которого рассчитывается показатель.

  Стандартное отклонение – показатель разброса значений активности за выбранный период.

Аномальная активность пользователя записывается в журнал, если значение одного из показателей (**Relative Score** или **Z-Score**) превышает заданный порог. Для каждого анализируемого признака правило выбирает наиболее подходящий показатель в зависимости от статистики поведения пользователя.

Использование двух индикаторов позволяет оценивать аномальное поведение в различных сценариях и уменьшает количество ложных срабатываний. При выявлении аномалии правило создает корреляционное событие, которое содержит информацию о пользователе, времени, анализируемом признаке, типе показателя, значении показателя, пороге, который был превышен, а также аномальные значения для анализа аномалии.

Управление объектами в хранилищах

В Kaspersky EDR Expert предусмотрена возможность хранения объектов для обработки. Например, можно загрузить файл, чтобы проверить его немедленно или в будущем; зараженный файл можно поместить на карантин, чтобы обеспечить безопасность, а если потребуется, в дальнейшем восстановить его.

Для каждого типа объектов предусмотрено свое *хранилище*. В интерфейсе консоли OSMP работа с хранилищами осуществляется в разделе **Операции**.

Загрузка файлов для проверки

Вы можете загрузить файл и проверить его сразу или позже. Kaspersky EDR Expert использует для проверки технологии Anti-Malware Engine и YARA, а также отправляет файл в Sandbox.

Чтобы загрузить файл для проверки:

1. В главном окне приложения перейдите в раздел **Операции** →**Хранилища** → **Файлы**.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно **Загрузить файл**.
3. Выберите тенант, который требуется связать с файлом.
4. Если файл необходимо проверить сразу после завершения загрузки, убедитесь, что переключатель **Проверить после загрузки** включен. Этот переключатель можно выключить и проверить файл позже.
5. Загрузите файл, перетащив его или нажав **Загрузить файл**. Вы можете загрузить несколько файлов.
6. Нажмите на кнопку **Загрузить**.

Kaspersky EDR Expert начинает загрузку файла. После завершения загрузки Kaspersky EDR Expert приступит к проверке, если включен переключатель **Проверить после загрузки**.

Проверка файлов в разделе Файлы вручную

Вы можете запустить проверку вручную, если файл не был проверен или если вы хотите проверить его повторно. Kaspersky EDR Expert использует для проверки технологии Anti-Malware Engine и YARA, а также отправляет файл в Sandbox.

Чтобы выполнить проверку файлов в разделе Файлы:

1. В главном окне приложения перейдите в раздел **Операции** →**Хранилища** → **Файлы**.
2. Выберите в списке файл или несколько файлов.
3. Нажмите на кнопку **Проверить** над списком.

Kaspersky EDR Expert начнет проверку выбранных файлов. Вы можете просмотреть статус проверки в столбце **Статус проверки**.

Просмотр статуса и результатов проверки

Чтобы просмотреть состояние и результаты проверки файлов, выполните действия в следующем порядке:

1. В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Files**.

   В столбце **Статус проверки** в списке файлов приводится основная информация о состоянии проверки и результатах:

   - **Не выполнялась**

     Файл еще не проверялся.

   - **Проверяется**

     Файл находится на проверке.

   - **Не обнаружено**

     Файл проверен, угроз не обнаружено.

   - **Обнаружено**

     Файл проверен, обнаружены угрозы.

2. Для получения более подробной информации о файле нажмите на имя этого файла.

   В открывшемся окне приводится информация о файле, в том числе подробные результаты проверки файла.

Загрузка файлов из разделов Карантин и Файлы резервного хранилища

Вы можете загрузить файлы из Карантина и Резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Чтобы сохранить копию файла из раздела Карантин или Файлы резервных копий на жесткий диск:

1. Выполните одно из следующих действий:

   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Карантин**.

   - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Файлы резервных копий**.

2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Скачать**.

Начнется загрузка.

Если вы выполнили действие из раздела **Карантин**, копия файла, помещенного в директорию карантина на клиентском устройстве, загружается на ваше устройство. Файл сохраняется в ZIP-архиве, защищенном паролем. Пароль для файла архива: infected.

Восстановление файлов из карантина

Если у вас есть основания полагать, что файл, помещенный на карантин, безопасен, вы можете восстановить файл на устройстве одним из следующих способов:

- Из раздела **Карантин** главного меню.
- Из результатов действия по реагированию **Поместить на карантин**.

Также можно настроить автоматический запуск этого действия при создании или изменении плейбука.

Восстановление файла из раздела Карантин

Для восстановления файла из раздела Карантин выполните действия в следующем порядке:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Карантин**.
2. Выполните одно из следующих действий:
   - Выберите файл, который нужно восстановить из карантина.

     Вы можете выбрать несколько файлов.
   - Нажмите на имя файла, который нужно восстановить из карантина.

   Откроется окно со сведениями файла.
3. Нажмите на кнопку **Восстановить** и подтвердите операцию.

   При необходимости в поле **Описании** вы можете написать комментарий перед подтверждением операции.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл будет восстановлен на устройстве, на котором ранее вы поместили его на карантин, и расположен по исходному пути (указанному на шаге 5 в сценарии Перемещение файлов в карантин). Иначе отображается сообщение об ошибке.

Восстановление файла из результатов действия по реагированию **Поместить на карантин**

Для восстановления файла из результатов действия по реагированию Поместить на карантин выполните действия в следующем порядке:

1. Откройте результат действия **Поместить на карантин** одним из следующих способов:

   - В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.

   - В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**. В столбце **Идентификатор** нажмите идентификатор алерта или инцидента, который включает актив или наблюдаемый объект, для которого вы выполнили действие по реагированию **Поместить на карантин**. В открывшихся деталях алерта или инцидента перейдите на вкладку **История**.

2. Для результата действия по реагированию **Поместить на карантин** в столбце **Статус действия** перейдите по ссылке **Успешно**.

3. В открывшемся окне сведений нажмите на кнопку **Восстановить** и подтвердите операцию.

4. При необходимости в поле **Описание** вы можете написать комментарий перед подтверждением операции.

   Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл будет восстановлен на устройстве, на котором ранее вы поместили его на карантин, и расположен по исходному пути (указанному на шаге 5 в сценарии Перемещение файлов в карантин). Иначе отображается сообщение об ошибке.

Просмотр результатов восстановления файла

Если на устройстве установлено приложение Kaspersky Endpoint Security с встроенным агентом, результат восстановления файла отображается в разделе **История реагирований**.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если восстановление файла выполнено успешно, отобразится сообщение **Успешно**. В противном случае отобразится сообщение **Ошибка** с информацией о причине ошибки.

Если требуется просмотреть Идентификатор запуска и JSON с результатом восстановления файла, перейдите на вкладку **Отладка данных**.

Удаление файлов из карантина

Для выполнения этого действия у вас должна быть одна из следующих ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.

Вы можете удалить зараженный файл из карантина на устройстве одним из следующих способов:

- Из раздела **Карантин** Консоли OSMP.
- Из результатов действия по реагированию **Поместить на карантин**.

Также можно настроить автоматический запуск этого действия при создании или изменении плейбука.

Удаление файла из раздела Карантин

Для удаления файла из раздела Карантин выполните действия в следующем порядке:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Карантин**.
2. Выполните одно из следующих действий:
   - Выберите файл, который нужно удалить из карантина.

     Вы можете выбрать несколько файлов.
   - Нажмите на имя файла, который нужно удалить из карантина.

     Откроется окно со сведениями файла.
3. Нажмите на кнопку **Удалить** и подтвердите операцию.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удален из карантина на устройстве, на котором он находился, без возможности восстановления. Иначе отображается сообщение об ошибке.

Для удаления файла из результатов действия по реагированию **Поместить на карантин** выполните действия в следующем порядке:

Для удаления файла из результатов действия по реагированию Поместить на карантин выполните действия в следующем порядке:

1. Откройте результат действия **Поместить на карантин** одним из следующих способов:
   - В главном окне приложения перейдите в раздел **Мониторинг** → **История реагирований**.
   - В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**. В столбце **Идентификатор** нажмите идентификатор алерта или инцидента, который включает актив или наблюдаемый объект, для которого вы выполнили действие по реагированию **Поместить на карантин**. В открывшихся деталях алерта или инцидента перейдите на вкладку **История**.

2. Для результата действия по реагированию **Поместить на карантин** в столбце **Статус действия** перейдите по ссылке **Успешно**.

3. В открывшемся окне сведений нажмите на кнопку **Удалить** и подтвердите операцию.

   Если операция завершена успешно, на экране отобразится соответствующее сообщение. Файл удален из карантина на устройстве, на котором он находился, без возможности восстановления. Иначе отображается сообщение об ошибке.

Просмотр результатов удаления файла

Если на устройстве установлено приложение Kaspersky Endpoint Security с встроенным агентом, результат удаления файла отображается в разделе **История реагирований**.

После того как вы перейдете по ссылке в столбце **Статус действия**, откроется окно с выбранной вкладкой **Результат**. Если удаление файла выполнено успешно, отобразится сообщение **Успешно**. В противном случае отобразится сообщение **Ошибка** с информацией о причине ошибки.

Если требуется просмотреть Идентификатор запуска и JSON с результатом удаления файла, перейдите на вкладку **Отладка данных**.

Об удалении объектов из разделов Карантин, Файлы резервного хранилища или Активные угрозы

Когда приложения безопасности "Лаборатории Касперского", установленные на клиентских устройствах, помещают объекты на Карантин, в Резервное хранилище или Активные угрозы, они передают информацию о добавленных объектах в разделы **Карантин**, **Файлы резервных копий** или **Активные угрозы** в Open Single Management Platform. При открытии одного из этих разделов, вы можете удалить нужный объект.

В разделе **Файлы резервных копий** или **Активные угрозы** выберите объект из списка и нажмите на кнопку **Удалить**.

В разделе **Карантин** можно выполнить одно из следующих действий:

- Установить флажок рядом с именем объекта, который нужно удалить, а затем в панели инструментов нажать на кнопку **Удалить**.

- Нажать на имя объекта, который нужно удалить, и в открывшемся окне свойств в панели инструментов нажать на кнопку **Удалить**.

  В этом случае объект будет удален, на экране отобразится соответствующее уведомление, окно со свойствами закроется.

Open Single Management Platform либо удаляет выбранный объект из списка, либо удаляет выбранный объект из хранилища. Действие, которое необходимо выполнить, определяется приложением "Лаборатории Касперского", поместившим выбранный объект в хранилище. Приложение "Лаборатории Касперского" указано в поле **Запись добавлена**.

Подробнее о том, какое действие нужно выполнить, см. справку приложения "Лаборатории Касперского".

Управление активами

Управление активами в Kaspersky EDR Expert предоставляет следующие возможности:

- Управление активами в KUMA: просмотр информации об активах, поиск активов, добавление, редактирование и удаление активов, а также экспорт данных об активах в CSV-файл.
- Запускать задачи и применять к активам политики приложения "Лаборатории Касперского" можно в разделе **Активы (Устройства)** интерфейса Консоли OSMP.
- Получить общую информацию об активах можно в виджете **Активы** на вкладке **Обнаружение и реагирование** на панели мониторинга Консоли OSMP.
- Сведения об активе приводятся в разделе **Мониторинг**.

Интеграция с другими решениями

Интеграция с другими решениями позволяет расширить функциональность Kaspersky EDR Expert.

Kaspersky EDR Expert поддерживает интеграцию со следующими решениями "Лаборатории Касперского":

- Kaspersky Managed Detection and Response
- Kaspersky Security Network
- Kaspersky Threat Intelligence Portal.

Интеграция с Kaspersky Managed Detection and Response

Решение Kaspersky Managed Detection and Response (далее также "MDR") предназначено для обнаружения и предотвращения мошеннических действий в инфраструктуре клиента. MDR обеспечивает непрерывную управляемую защиту и позволяет организациям автоматически выявлять труднообнаружимые угрозы и освобождать сотрудников группы IT-безопасности для решения задач, требующих их участия.

Если в OSMP включен MDR, доступно только создание инцидентов MDR из инцидентов Open Single Management Platform.

Если в MDR включена отправка данных из Open Single Management Platform в MDR, в SOC MDR также поступает дополнительная информация об обнаружении. Для этого требуется дополнительное согласие клиента MDR в плагине MDR.

Вы можете создать инцидент Kaspersky Managed Detection and Response из инцидента EDR, если алерты инцидента соответствуют следующим условиям:

- В OSMP включена интеграция с MDR
- Источником обнаружения является конечная точка
- Включен хотя бы один связанный актив
- Технология обнаружения может быть любой из следующих:
  - IOA-правила
  - SB (Sandbox)
  - AM (Anti-Malware Engine)
  - YARA
  - IOC

Подробные сведения приведены в документации Kaspersky Managed Detection and Response.

Интеграция с Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky EDR Expert использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky EDR Expert на объекты, информация о которых еще не вошла в базы антивирусных приложений, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных приложений, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний приложения, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky EDR Expert отправляет запросы в Kaspersky Security Network о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Сбор, обработка и хранение персональных данных пользователя не осуществляется. О данных, которые Kaspersky EDR Expert передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. Вы можете начать использование KSN или отказаться от использования KSN в любой момент.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также KPSN). KPSN – это решение, которое позволяет пользователям получать доступ к репутационным базам Kaspersky Security Network и другим статистическим данным без отправки данных со своих компьютеров в Kaspersky Security Network.

По вопросам приобретения приложения Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

Чтобы настроить доступ Сервера администрирования к KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования [Включено]**.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Open Single Management Platform не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Open Single Management Platform). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Open Single Management Platform) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network [Включено]**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network [Включено]** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями .pkcs7 и .pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

   При переводе переключателя в положение **Использовать Kaspersky Private Security Network [Включено]** появится сообщение с подробной информацией о KPSN.

   KPSN поддерживают следующие приложения "Лаборатории Касперского":

   - Open Single Management Platform
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   Если вы включите KPSN в Open Single Management Platform, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

   > Open Single Management Platform не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **KSN Proxy settings**.

5. Установите флажок **Игнорировать параметры прокси-сервера, настроенные в KSC, для подключения к KPSN**, если в свойствах Сервера администрирования настроены параметры прокси-сервера, но архитектура сети требует работы с KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. В блоке параметров **Параметры подключения** настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - TCP-порт 13111 используется для подключения к прокси-серверу KSN. Для корневого Сервера администрирования этот номер порта изменить невозможно.

   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт**. По умолчанию параметр выключен, используется порт TCP. Если этот параметр включен, по умолчанию используется UDP-порт 15111. Для корневого Сервера администрирования этот номер порта изменить невозможно.

7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер [Включено]**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   > Подчиненные Серверы администрирования используют в качестве прокси-сервера главный Сервер администрирования, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования [Включено]**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.

2. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Общие** выберите раздел **Точки распространения**.

4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.

5. В окне свойств точки распространения в разделе **Прокси-сервер KSN** включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

6. Нажмите на кнопку **OK**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Обратите внимание, что точка распространения не поддерживает проверку подлинности управляемого устройства по протоколу NTLM.

Включение и отключение участия в KSN и KPSN

Пользователи со следующими ролями могут просматривать и редактировать статус участия в Kaspersky Security Network и Kaspersky Private Security Network:

- Главный администратор
- Администратор SOC
- Администратор тенанта (изменение статуса доступно только для корневого клиента – для остальных тенантов в иерархии настройки применяются автоматически)

Пользователи с ролью Аудитор могут только просматривать статус участия в Kaspersky Security Network и Kaspersky Private Security Network.

Чтобы включить участие в Kaspersky Security Network:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.
2. В разделе **Kaspersky EDR Expert** выберите режим подключения **KSN**.
3. Включите переключатель **Участие в KSN**.
4. Внимательно прочитайте Положение о KSN.
5. Если вы согласны с условиями Положения о KSN, выберите параметр **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения документа Положение о KSN** и нажмите **Принять**.

   KSN будет включен, и Open Single Management Platform будет отправлять статистические данные в KSN для анализа специалистами "Лаборатории Касперского".

6. Если вы не согласны с условиями Положения о KSN, нажмите **Отклонить**.

   KSN не будет включена.

Чтобы включить участие в Kaspersky Private Security Network:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.
2. В разделе **Kaspersky EDR Expert** выберите режим подключения **KPSN**.

3. Включите переключатель **Участие в KPSN**.

4. Нажмите на кнопку **Загрузить**, выберите файл конфигурации KPSN (файл с расширением pkcs7 или pem) и нажмите **Открыть**.

Участие в KPSN включено.

Чтобы отключить участие в KSN или KPSN, выполните действия в следующем порядке:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.

2. Если вы хотите отключить участие в KSN, выберите режим подключения **KSN** и выключите переключатель **Участие в KSN**.

   Участие в KSN отключено.

3. Если вы хотите отключить участие в KPSN, выберите режим подключения **KPSN** и выключите переключатель **Участие в KPSN**.

   Участие в KPSN отключено.

Настройка подключения к локальной репутационной базе KPSN

Kaspersky EDR Expert может сохранять информацию об алертах, созданных компонентом Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для устройств локальной сети организации.

Приложение позволяет пользователям со следующими ролями просматривать и изменять параметры интеграций API Kaspersky Private Security Network:

- Главный администратор
- Администратор SOC
- Администратор тенанта (изменение параметров иерархии доступно только для корневого тенанта, для остальных тенантов в иерархии параметры применяются автоматически)

Пользователи с ролью Аудитор может только просматривать параметры интеграции API Kaspersky Private Security Network.

Чтобы настроить подключение Kaspersky EDR Expert к локальной репутационной базе KPSN:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на **Тенант Root** и перейдите в подраздел **Параметры** → **Репутационные базы KPSN**.

3. В поле **Актив** укажите IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN.

4. Нажмите **Загрузить** справа от поля **Открытый ключ для пользовательского сертификата** и выберите нужный сертификат .pem.

5. Нажмите **Загрузить** справа от поля **Закрытый ключ для пользовательского сертификата** и выберите нужный сертификат .pem.

6. Нажмите **Загрузить** справа от поля **Доверенный корневой сертификат для сервера KPSN** и выберите нужный сертификат .pem.

7. Нажмите на кнопку **Сохранить**.

Подключение к локальной репутационной базе KPSN настроено.

Настройка отправки обнаруженных объектов в список запрещенных KPSN

Приложение позволяет пользователям с ролями Аналитик 1-го уровня и Аналитик 2-го уровня включать или выключать автоматическую отправку хешей вредоносных файлов, просканированных Sandbox, в список запрещенных KPSN. Конфигурация этого параметра отличается для каждого тенанта. Параметр можно изменить только в корневом тенанте установки OSMP – в дочерних тенантах параметр изменить нельзя.

Перед включением автоматической отправки обнаруженных объектов в список запрещенных KPSN убедитесь, что использование KPSN включено и настроено подключение к локальной репутационной базе KPSN.

Чтобы включить автоматическую отправку обнаруженных объектов в список запрещенных KPSN:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на **Тенант Root** и перейдите в подраздел **Параметры** → **Репутационные базы KPSN**.

3. Включите переключатель **Присвоить объектам статус Недоверенный**.

4. Нажмите на кнопку **Сохранить**.

Просмотр Положения о Kaspersky Security Network

При включении Kaspersky Security Network необходимо прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Интеграция с Kaspersky Threat Intelligence Portal

Портал Kaspersky Threat Intelligence Portal объединяет все знания "Лаборатории Касперского" о киберугрозах и их взаимосвязи в единую веб-службу. При интеграции с Kaspersky EDR Expert он помогает пользователям быстрее принимать обоснованные решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, данных WHOIS / DNS.

Доступ к Kaspersky TIP предоставляется на платной основе. Лицензионные сертификаты создаются специалистами "Лаборатории Касперского". Чтобы получить сертификат для Kaspersky TIP, обратитесь к вашему персональному техническому менеджеру "Лаборатории Касперского".

Перед настройкой параметров вам необходимо создать токен авторизации для API-запросов на Kaspersky TIP или Kaspersky OpenTIP.

Для настройки интеграции между Open Single Management Platform и Kaspersky TIP:

1. На вкладке **Общие** выберите раздел **Тенанты**.

   Отобразится список тенантов.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Параметры** и выберите раздел **Kaspersky TIP**.

   Вы можете изменить значения в разделе **Kaspersky TIP**, если вам назначена одна из следующих ролей: Главный администратор, Администратор тенанта или Администратор SOC.

4. Если на шаге 2 выбран корневой тенант, с помощью переключателя **Прокси-сервер** можно включить использование прокси-сервера для взаимодействия с Kaspersky TIP.

   Прокси-сервер настраивается в свойствах корневого Сервера администрирования.

5. В поле **TTL кеш** укажите срок хранения кеша и единицы измерения: дни или часы.

   По умолчанию установлено 7 дней. Если вы не укажете никакого значения, срок хранения кеша неограничен.

   Вы устанавливаете период хранения кеша для всех подключений.

6. Включите переключатель **Интеграция** для одной из следующих служб:

   - **Kaspersky Threat Intelligence Portal (общий доступ)**

     После добавления токена авторизации вы сможете получить информацию от Kaspersky TIP о следующих типах объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обогащение**. При запросе данных расходуется квота данных.

- Kaspersky Threat Intelligence Portal (премиум-доступ)

  После добавления токена авторизации вы сможете выполнять следующие действия:

  - Получать подробную информацию от Kaspersky TIP о следующих типах наблюдаемых объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обогащение**. При запросе данных расходуется квота данных.

  - Получать подробную информацию от Kaspersky TIP о следующих типах наблюдаемых объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обновление статуса**. При запросе данных квота не расходуется.

7. Нажмите на кнопку **Добавить токен**.

8. В открывшемся окне введите нужные данные токена авторизации и нажмите на кнопку **Добавить**.

   Подробнее о формировании токена авторизации для API-запросов см. в справке Kaspersky TIP или Kaspersky OpenTIP.

   После добавления токена вы можете заменить его, нажав на кнопку **Заменить** и введя новый токен в открывшемся окне. Это может быть необходимо, если срок действия токена истек.

9. Нажмите на кнопку **Сохранить**.

Взаимодействие с НКЦКИ

Kaspersky EDR Expert позволяет вам взаимодействовать с Национальным координационным центром по компьютерным инцидентам (далее НКЦКИ). Субъект ГосСОПКА, который использует Kaspersky EDR Expert, может передавать данные о компьютерных инцидентах, обнаруженных компьютерных атаках и уязвимостях, используя экспорт инцидентов в НКЦКИ. Благодаря обмену информацией об инцидентах, реагирование на компьютерные инциденты, которые происходят на субъектах критической информационной инфраструктуры Российской Федерации, может стать более оперативным.

В Kaspersky EDR Expert в рамках взаимодействия с НКЦКИ можно выполнять следующие действия:

- экспортировать в НКЦКИ инциденты;

- просматривать изменения в параметрах экспортированных инцидентов, сделанные в НКЦКИ.

Условия взаимодействия с НКЦКИ

Для взаимодействия с НКЦКИ должны выполняться следующие условия:

- Лицензия приложения включает модуль GosSOPKA.

- Настроена интеграция с НКЦКИ.

- Пользователю, который работает с инцидентами НКЦКИ должна быть присвоена одна из следующих предопределенных ролей:
  - Главный администратор.
  - Администратор тенанта.
  - Работа с НКЦКИ.

Этапы взаимодействия с НКЦКИ

В Kaspersky EDR Expert процесс подготовки и обработки инцидентов НКЦКИ состоит из следующих этапов:

1. **Создание инцидента и проверка его на соответствие требованиям НКЦКИ**

   Вы можете создать инцидент НКЦКИ на основе инцидента XDR. Перед отправкой данных в НКЦКИ убедитесь, что категория инцидента соответствует требованиям НКЦКИ.

2. **Экспорт инцидента в НКЦКИ**

   При успешном экспорте инцидента в НКЦКИ, статус инцидента принимает значение *Отправлен в НКЦКИ*.

   В НКЦКИ полученному инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**.

   Статус инцидента и некоторые параметры инцидента могут обновляться на стороне НКЦКИ. Если сотрудники НКЦКИ внесли изменения, значения параметров инцидента НКЦКИ обновляются. Данные между Kaspersky EDR Expert и НКЦКИ синхронизируются каждые 5–10 минут. Если в НКЦКИ предоставлены все необходимые данные, инциденту присваивается статус *Проверка НКЦКИ*.

3. **Завершение обработки инцидента**

   Когда сотрудники НКЦКИ обработают инцидент, в НКЦКИ ему будет присвоен статус *Принято решение*. В Kaspersky EDR Expert этот статус отображается в заголовке окна со сведениями об инциденте НКЦКИ.

   При получении статуса *Отправлен в архив* взаимодействие с НКЦКИ по инциденту через Kaspersky EDR Expert становится невозможным. При этом закрытые инциденты можно найти в таблице инцидентов НКЦКИ и просмотреть сведения о них.

Настройка интеграции с НКЦКИ

Вы можете создать подключение к НКЦКИ. Это позволит вам экспортировать в него инциденты, зарегистрированные в Kaspersky EDR Expert.

Чтобы настроить интеграцию с НКЦКИ:

1. В главном меню перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть доступ на чтение.

2. Нажмите на имя требуемого тенанта.

   Откроется окно свойств тенанта. Если у вас есть только право доступа на чтение к этому тенанту, свойства будут доступны только для чтения. Если у вас есть право доступа на запись, вы можете настроить свойства тенанта.

3. В окне свойств тенанта перейдите на вкладку **Параметры** и в разделе **Сторонние интеграции** выберите **НКЦКИ**.

4. Включите опцию **Интеграция с НКЦКИ**.

5. В поле **URL** введите URL, по которому доступен НКЦКИ. Например: `https://example.cert.gov.ru/api/v2/`.

6. В поле **API-токен** нажмите на кнопку **Добавить токен** и задайте API-токен вручную.

7. В поле **Организация** укажите название вашей компании. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

8. В раскрывающемся списке **Функция затронутой системы** выберите сферу, в которой работает ваша организация. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

   Доступные сферы деятельности компании

   - Атомная энергетика.
   - Банковская сфера и иные сферы финансового рынка.
   - Горнодобывающая промышленность.
   - Государственная/муниципальная власть.
   - Здравоохранение.
   - Металлургическая промышленность.
   - Наука.
   - Оборонная промышленность.
   - Образование.
   - Ракетно-космическая промышленность.
   - Связь.
   - СМИ.
   - Топливно-энергетический комплекс.
   - Транспорт.
   - Химическая промышленность.
   - Иная.

9. В раскрывающемся списке **Расположение** выберите геокод, соответствующий субъекту Российской Федерации, в котором располагается ваша компания. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

   Список геокодов Российской Федерации

Список геокодов Российской Федерации

Субъект РФ	Геокод
Адыгея	RU-AD
Алтайский край	RU-ALT
Амурская область	RU-AMU
Архангельская область	RU-ARK
Астраханская область	RU-AST
Башкортостан	RU-BA
Белгородская область	RU-BEL
Брянская область	RU-BRY
Бурятия	RU-BU
Владимирская область	RU-VLA
Волгоградская область	RU-VGG
Вологодская область	RU-VLG
Воронежская область	RU-VOR
Дагестан	RU-DA
Еврейская автономная область	RU-YEV
Забайкальский край	RU-ZAB
Ивановская область	RU-IVA
Ингушетия	RU-IN
Иркутская область	RU-IRK
Кабардино-Балкария	RU-KB
Калининградская область	RU-KGD
Калмыкия	RU-KL
Калужская область	RU-KLU
Камчатский край	RU-KAM
Карачаево-Черкессия	RU-KC
Карелия	RU-KR
Кемеровская область	RU-KEM
Кировская область	RU-KIR
Костромская область	RU-KOS
Краснодарский край	RU-KDA
Красноярский край	RU-KYA
Курганская область	RU-KGN
Курская область	RU-KRS
Ленинградская область	RU-LEN
Липецкая область	RU-LIP
Магаданская область	RU-MAG
Марий Эл	RU-ME
Мордовия	RU-MO
Москва	RU-MOW
Московская область	RU-MOS

Субъект РФ	Геокод
Мурманская область	RU-MUR
Ненецкий автономный округ	RU-NEN
Нижегородская область	RU-NIZ
Новгородская область	RU-NGR
Новосибирская область	RU-NVS
Омская область	RU-OMS
Оренбургская область	RU-ORE
Орловская область	RU-ORL
Пензенская область	RU-PNZ
Пермский край	RU-PER
Приморский край	RU-PRI
Псковская область	RU-PSK
Республика Алтай	RU-AL
Республика Коми	RU-KO
Республика Саха	RU-SA
Ростовская область	RU-ROS
Рязанская область	RU-RYA
Самарская область	RU-SAM
Санкт-Петербург	RU-SPE
Саратовская область	RU-SAR
Сахалинская область	RU-SAK
Свердловская область	RU-SVE
Северная Осетия	RU-SE
Смоленская область	RU-SMO
Ставропольский край	RU-STA
Тамбовская область	RU-TAM
Татарстан	RU-TA
Тверская область	RU-TVE
Томская область	RU-TOM
Тульская область	RU-TUL
Тыва	RU-TY
Тюменская область	RU-TYU
Удмуртия	RU-UD
Ульяновская область	RU-ULY
Хабаровский край	RU-KHA
Хакасия	RU-KK
Ханты-Мансийский автономный округ – Югра	RU-KHM
Челябинская область	RU-CHE
Чечня	RU-CE
Чувашия	RU-CU
Чукотский автономный округ	RU-CHU

Субъект РФ	Геокод
Ямало-Ненецкий автономный округ	RU-YAN
Ярославская область	RU-YAR

10. Включите опцию **Использовать прокси-сервер**, чтобы подключаться к НКЦКИ через прокси-сервер.

    Нажмите на ссылку **Параметры**, чтобы задать настройки прокси-сервера. Откроется окно свойств Сервера администрирования, в котором вы можете выполнить настройку.

11. Вы можете указать следующие параметры об операторе персональных данных в соответствующих полях:

    - **Наименование**
    - **ИНН**
    - **Адрес**
    - **Адрес электронной почты**

    Вы также можете убедиться, что соединение с НКЦКИ установлено, нажав на кнопку **Проверить подключение**. Статус проверки отобразится в поле **Статус подключения**.

12. Нажмите на кнопку **Сохранить** для завершения настройки интеграции.

Kaspersky EDR Expert интегрирован с НКЦКИ. Теперь вы можете экспортировать в него инциденты.

Чтобы выключить интеграцию с НКЦКИ:

1. В главном меню перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть доступ на чтение.

2. Нажмите на имя требуемого тенанта.

   Откроется окно свойств тенанта. Если у вас есть только право доступа на чтение к этому тенанту, свойства будут доступны только для чтения. Если у вас есть право доступа на запись, вы можете настроить свойства тенанта.

3. В окне свойств тенанта перейдите на вкладку **Параметры** и в разделе **Сторонние интеграции** выберите **НКЦКИ**.

4. Выключите опцию **Интеграция с НКЦКИ**.

5. Нажмите на кнопку **Сохранить**.

Интеграция Kaspersky EDR Expert с НКЦКИ выключена.

Просмотр таблицы инцидентов НКЦКИ

Таблица инцидентов НКЦКИ содержит информацию обо всех созданных инцидентах НКЦКИ.

Чтобы просмотреть таблицу инцидентов НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

2. При необходимости отфильтруйте тенанты. По умолчанию фильтр тенантов выключен и в таблице инцидентов отображаются инциденты, относящиеся ко всем тенантам, к которым у вас есть права доступа. Чтобы применить фильтр для тенантов:

   a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

      Откроется список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

      В таблице инцидентов отображаются только инциденты, обнаруженные на активах, принадлежащих выбранным тенантам.

3. Выберите вкладку **Инциденты НКЦКИ**.

   Откроется таблица с инцидентами НКЦКИ. Таблица содержит следующие столбцы:

   - **Короткий идентификатор** – уникальный идентификатор инцидента НКЦКИ.
   - **Тенант** – имя тенанта, в котором был обнаружен инцидент.
   - **Обнаружен** – дата и время обнаружения инцидента.
   - **Завершен** – дата и время закрытия инцидента.
   - **Статус** – текущий статус инцидента НКЦКИ, экспортированного в НКЦКИ.
   - **Категория** – категория инцидента НКЦКИ.
   - **Тип** – тип инцидента НКЦКИ.

4. Вы можете группировать и фильтровать данные таблицы с инцидентами НКЦКИ. Для этого нажмите на значок параметров (⚙) или на значок фильтрации (▽) в правом верхнем углу таблицы и настройте параметры отображения инцидентов.

   По умолчанию таблица инцидентов НКЦКИ отфильтрована по столбцу **Статус**: инциденты со статусом *Отправлен в архив* и *Принято решение* не отображаются.

Просмотр сведений об инциденте НКЦКИ

В окне со сведениями об инциденте НКЦКИ вы можете просматривать всю информацию, относящуюся к инциденту, включая его свойства.

Чтобы просмотреть сведения об инциденте НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

2. Выберите вкладку **Инциденты НКЦКИ**.

3. В открывшейся таблице нажмите на идентификаторинцидента.

Откроется окно со сведениями об инциденте НКЦКИ.

В заголовке окна указан краткий уникальный идентификатор инцидента и статус, присвоенный инциденту в НКЦКИ. Если инцидент еще не был экспортирован в НКЦКИ, он имеет статус *Черновик*. Некоторые параметры инцидента НКЦКИ доступны для редактирования, остальные параметры наследуются от инцидента XDR и не редактируются.

При необходимости вы можете обновить информацию в окне со сведениями об инциденте, нажав на значок ⟲ рядом с заголовком окна.

С помощью панели инструментов в верхней части окна вы можете выполнять следующие действия:

- редактировать инцидент НКЦКИ;
- удалять инцидент НКЦКИ;
- экспортировать инцидент НКЦКИ.

Окно сведений об инциденте НКЦКИ содержит разделы, описанные ниже.

Сводная информация

В этом разделе вы можете просматривать и при необходимости редактировать следующую общую информацию об инциденте НКЦКИ:

- **Короткий идентификатор** – уникальный идентификатор инцидента НКЦКИ.
- **Тенант** – имя тенанта, в котором был обнаружен инцидент.
- **Обнаружено** – дата и время обнаружения инцидента.
- **Завершено** – дата и время закрытия инцидента. Этот параметр доступен для редактирования.
- **Описание** – краткое описание инцидента. Этот параметр доступен для редактирования.
- **Категория** – категория инцидента НКЦКИ. Этот параметр доступен для редактирования.
- **Тип** – тип инцидента НКЦКИ. Этот параметр доступен для редактирования.
- **Утечка персональных данных** – уведомление об утечке персональных данных. Этот параметр доступен для редактирования.

  Параметр отображается, если при редактировании категории инцидента вы выбрали **Уведомление о компьютерном инциденте**, а затем выбрали один из следующих типов:

  - **Заражение ВПО**
  - **Компрометация учетной записи**
  - **Несанкционированное разглашение информации**
  - **Успешная эксплуатация уязвимости**
  - **Событие не связано с компьютерной атакой**

Доступные поля

Уведомление об утечке персональных данных – включите этот переключатель в случае утечки персональных данных, после чего раздел **Утечка персональных данных** станет доступным.

Оператор персональных данных – наименование опрератора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

ИНН – ИНН оператора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

Адрес – адрес опрератора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

Адрес электронной почты – адрес электронной почты опрератора персональных данных для отправки информации об уведомлении. Поле отображается, если настроена интеграция с НКЦКИ.

Причины, повлекшие нарушение прав субъектов персональных данных – укажите причины, повлекшие нарушение прав субъектов персональных данных.

Характеристики персональных данных – укажите характеристики персональных данных.

Предполагаемый вред, нанесенный правам субъектов персональных данных – укажите, какой вред нанесен правам субъектов персональных данных.

Принятые меры по устранению последствий инцидента.

Дополнительные сведения.

Информация о результатах внутреннего расследования инцидента.

- **Название компании** – наименование главной организации, в которой произошел инцидент.
- **TLP** – маркер протокола Traffic Light, который определяет уровень конфиденциальности информации, содержащейся в сведениях об инциденте НКЦКИ. Этот параметр доступен для редактирования.

  Возможные значения маркера

  - **WHITE** – раскрытие не ограничено.
  - **GREEN** – раскрытие только для сообщества.
  - **AMBER** – раскрытие только для организаций.
  - **RED** – раскрытие только для круга лиц.
- **Состояние действия** – статус реагирования на инцидент. Этот параметр доступен для редактирования.

  Возможные значения статуса

  Значения статуса по умолчанию заполняются по таблице соответствий приведенной ниже.

Список статусов инцидентов XDR и соответствующих статусов реагирования

Статус инцидента XDR	Статус реагирования инцидента НКЦКИ
Новый, В процессе, Отложен	Проводятся мероприятия по реагированию
Закрыт как: истинноположительный результат	Меры приняты

Статус инцидента XDR	Статус реагирования инцидента НКЦКИ
Закрыт как: • ложное срабатывание; • низкоприоритетный; • объединен.	Инцидент не подтвержден

- **Инцидент XDR** – инцидент XDR, на основе которого был создан инцидент НКЦКИ.

- **Затронутая система имеет подключение к интернету** – наличие доступа в интернет в системе, где произошел инцидент. Этот параметр доступен для редактирования.

  Если система, где произошел инцидент, имеет доступ в интернет, то становится доступна вкладка, где можно заполнить технические сведения об атакованном ресурсе (раздел **Технические сведения об атакованном ресурсе**) и вредоносной системе (раздел **Технические сведения о вредоносной системе**).

- **Требуется помощь** – необходимость получения помощи от сотрудников НКЦКИ. Этот параметр доступен для редактирования.

- **Имя затронутой системы** – название атакованной системы. Этот параметр доступен для редактирования.

- **Категория затронутой системы** – категория значимости объекта критической информационной инфраструктуры (далее КИИ). Этот параметр доступен для редактирования.

  Список категорий значимости

  Объекты КИИ имеют следующие категории значимости:

  - объект КИИ первой категории значимости;
  - объект КИИ второй категории значимости;
  - объект КИИ третьей категории значимости;
  - объект КИИ без категории значимости;
  - информационный ресурс не является объектом КИИ.

- **Функция затронутой системы** – сфера деятельности организации, в которой функционирует атакованная система.

  Доступные сферы деятельности компании

  - Атомная энергетика.
  - Банковская сфера и иные сферы финансового рынка.
  - Горнодобывающая промышленность.
  - Государственная/муниципальная власть.
  - Здравоохранение.
  - Металлургическая промышленность.
  - Наука.
  - Оборонная промышленность.

- Образование.
- Ракетно-космическая промышленность.
- Связь.
- СМИ.
- Топливно-энергетический комплекс.
- Транспорт.
- Химическая промышленность.
- Иная.

- **Расположение** – геокод, соответствующий субъекту Российской Федерации, в котором располагается организации.

  Список геокодов Российской Федерации

Список геокодов Российской Федерации

Субъект РФ	Геокод
Адыгея	RU-AD
Алтайский край	RU-ALT
Амурская область	RU-AMU
Архангельская область	RU-ARK
Астраханская область	RU-AST
Башкортостан	RU-BA
Белгородская область	RU-BEL
Брянская область	RU-BRY
Бурятия	RU-BU
Владимирская область	RU-VLA
Волгоградская область	RU-VGG
Вологодская область	RU-VLG
Воронежская область	RU-VOR
Дагестан	RU-DA
Еврейская автономная область	RU-YEV
Забайкальский край	RU-ZAB
Ивановская область	RU-IVA
Ингушетия	RU-IN
Иркутская область	RU-IRK
Кабардино-Балкария	RU-KB
Калининградская область	RU-KGD
Калмыкия	RU-KL
Калужская область	RU-KLU
Камчатский край	RU-KAM
Карачаево-Черкессия	RU-KC

Субъект РФ	Геокод
Карелия	RU-KR
Кемеровская область	RU-KEM
Кировская область	RU-KIR
Костромская область	RU-KOS
Краснодарский край	RU-KDA
Красноярский край	RU-KYA
Курганская область	RU-KGN
Курская область	RU-KRS
Ленинградская область	RU-LEN
Липецкая область	RU-LIP
Магаданская область	RU-MAG
Марий Эл	RU-ME
Мордовия	RU-MO
Москва	RU-MOW
Московская область	RU-MOS
Мурманская область	RU-MUR
Ненецкий автономный округ	RU-NEN
Нижегородская область	RU-NIZ
Новгородская область	RU-NGR
Новосибирская область	RU-NVS
Омская область	RU-OMS
Оренбургская область	RU-ORE
Орловская область	RU-ORL
Пензенская область	RU-PNZ
Пермский край	RU-PER
Приморский край	RU-PRI
Псковская область	RU-PSK
Республика Алтай	RU-AL
Республика Коми	RU-KO
Республика Саха	RU-SA
Ростовская область	RU-ROS
Рязанская область	RU-RYA
Самарская область	RU-SAM
Санкт-Петербург	RU-SPE
Саратовская область	RU-SAR
Сахалинская область	RU-SAK
Свердловская область	RU-SVE
Северная Осетия	RU-SE
Смоленская область	RU-SMO
Ставропольский край	RU-STA
Тамбовская область	RU-TAM

Субъект РФ	Геокод
Татарстан	RU-TA
Тверская область	RU-TVE
Томская область	RU-TOM
Тульская область	RU-TUL
Тыва	RU-TY
Тюменская область	RU-TYU
Удмуртия	RU-UD
Ульяновская область	RU-ULY
Хабаровский край	RU-KHA
Хакасия	RU-KK
Ханты-Мансийский автономный округ – Югра	RU-KHM
Челябинская область	RU-CHE
Чечня	RU-CE
Чувашия	RU-CU
Чукотский автономный округ	RU-CHU
Ямало-Ненецкий автономный округ	RU-YAN
Ярославская область	RU-YAR

- **Средство обнаружения** – приложение, с помощью которого был зарегистрирован инцидент. Этот параметр доступен для редактирования.

- **Город** – город, в котором расположен объект КИИ, на котором произошел инцидент, атака или обнаружена уязвимость. Этот параметр доступен для редактирования.

- **Влияние на доступность** – влияние инцидента на доступность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Влияние на целостность** – влияние инцидента на целостность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Влияние на конфиденциальность** – влияние инцидента на конфиденциальность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Другое влияние** – описание других последствий компьютерного инцидента или компьютерной атаки.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Категория программ** – наименование и версия уязвимого приложения. Параметр доступен для категории инцидента НКЦКИ *Уведомление о наличии уязвимости*.

- **Технические сведения об атакованном ресурсе** – технические сведения о системе, где произошел инцидент, атака или обнаружена уязвимость. Этот параметр доступен для редактирования.

  Список параметров атакованного ресурса

  При наличии доступа в интернет в системе, где произошел инцидент, становится доступна вкладка, где можно заполнить технические сведения об атакованном ресурсе. Параметры раздела доступны к заполнению в зависимости от категории и типа инцидента НКЦКИ (см. таблицу ниже).

Параметры раздела **Технические сведения об атакованном ресурсе**

Название и описание параметра	Категория	Тип
IPv4-адрес IPv4-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
IPv6-адрес IPv6-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Имя домена Доменное имя контролируемого ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Социальная инженерия
URI-адрес URI-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Электронная почта	Уведомление о компьютерном	• Заражение ВПО

Название и описание параметра	Категория	Тип
Адрес электронной почты атакованного ресурса	инциденте	• Компрометация учетной записи • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Социальная инженерия
Атакуемый сетевой сервис Имя и порт/протокол атакованной сетевой службы	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости • Событие не связано с компьютерной атакой
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
AS-Path до атакованной автономной системы (ASN)	Уведомление о компьютерном инциденте	Захват сетевого трафика

- **Технические сведения о вредоносной системе** – технические сведения о вредоносной системе, вследствие атаки которой произошел инцидент. Этот параметр доступен для редактирования.

  Список параметров вредоносной системы

  При наличии доступа в интернет в системе, где произошел инцидент, становится доступна вкладка, где можно заполнить технические сведения о вредоносной системе. Параметры раздела доступны к заполнению в зависимости от категории и типа инцидента НКЦКИ (см. таблицу ниже).

Название и описание параметра	Категория	Тип
IPv4-адрес IPv4-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
IPv6-адрес IPv6-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Имя домена Доменное имя контролируемого ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации

Название и описание параметра	Категория	Тип
		• Сетевое сканирование • Социальная инженерия
URI-адрес URI-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Использование контролируемого ресурса для фишинга • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Социальная инженерия

Название и описание параметра	Категория	Тип
Функции – тип активности Предлагается к заполнению, если заполнено одно из полей **IPv4-адрес**, **IPv6-адрес**, **Имя домена** или **URI-адрес**. Возможные значения: • **Центр управления ВПО**. • **Элемент инфраструктуры ВПО**. • **Источник распространения ВПО**. • **Тип не определен**.	—	—
Электронная почта Адрес электронной почты атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Несанкционированное разглашение информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Социальная инженерия
Хеш вредоносного ПО Хеш-сумма вредоносного модуля	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО
Используемые уязвимости Описание используемых уязвимостей	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Номер автономной системы (ASN) Номер подставной автономной системы (ASN)	Уведомление о компьютерном инциденте	Захват сетевого трафика
Наименование AS Наименование подставной автономной системы	Уведомление о компьютерном инциденте	Захват сетевого трафика
Наименование LIR Наименование локального интернет-регистратора	Уведомление о компьютерном инциденте	Захват сетевого трафика

Интеграция с НКЦКИ

В этом разделе вы можете просматривать следующую информацию об инциденте, который был экспортирован в НКЦКИ:

- **UUID** – уникальный идентификатор карточки уведомления в НКЦКИ.
- **Регистрационный номер** – регистрационный номер уведомления в НКЦКИ.
- **Зарегистрировано** – дата и время регистрации инцидента в НКЦКИ.
- **Время обновления** – дата последнего обновления инцидента в НКЦКИ.

История

В этом разделе вы можете просматривать следующую информацию об истории изменений инцидента НКЦКИ:

- **Время** – дата и время изменения инцидента.
- **Пользователь** – имя пользователя, который изменил инцидент.
- **Подробнее** – информация об изменении инцидента.

Создание инцидента НКЦКИ

Вы можете создать инцидент НКЦКИ только на основе существующего инцидента XDR.

Чтобы создать инцидент НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Нажмите на инцидент XDR, на основе которого вы хотите создать инцидент для отправки в НКЦКИ. Инцидент XDR может иметь любой статус.

   Откроется окно со сведениями об инциденте XDR.
3. В панели управления в верхней части окна нажмите **Создать инцидент НКЦКИ**.

   Откроется окно создание инцидента НКЦКИ.
4. Заполните следующие поля:
   - **Категория** – категория инцидента НКЦКИ.
   - **Тип** – тип инцидента НКЦКИ.

5. При необходимости в поле **Активы** вы можете выбрать или добавить активы, вовлеченные в инцидент НКЦКИ. В таблице активов у таких устройств в столбце **Имеет признаки** стоит значение "атакующий" или "жертва".

   Данные о выбранных атакованных устройствах и вредоносных системах будут отображаться в окне со сведениями об инциденте НКЦКИ в разделах инцидента **Технические сведения об атакованном ресурсе** и **Технические сведения о вредоносной системе**.

Инцидент НКЦКИ создан. После этого в инцидент XDR добавляется ссылка на созданный инцидент НКЦКИ, а в инциденте НКЦКИ – ссылка на инцидент XDR. Вы можете просмотреть сведения об инциденте, отредактировать их и экспортировать инцидент в НКЦКИ.

Передача инцидентов в НКЦКИ

Чтобы экспортировать инцидент в НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

2. Выберите вкладку **Инциденты НКЦКИ**.

3. В открывшейся таблице нажмите на идентификатор инцидента НКЦКИ, который вы хотите экспортировать.

   Откроется окно со сведениями об инциденте.

   Если в списке инцидентов НКЦКИ отсутствует инцидент, который необходимо экспортировать, вы можете создать новый инцидент НКЦКИ.

4. При необходимости вы можете отредактировать параметры инцидента НКЦКИ перед экспортом. Для этого нажмите на кнопку **Изменить** в панели в верхней части окна инцидента НКЦКИ, заполните необходимые поля и сохраните изменения.

5. Нажмите на кнопку **Отправить в НКЦКИ** в панели в верхней части окна инцидента НКЦКИ.

6. В открывшемся окне подтвердите отправку инцидента в НКЦКИ.

Запрос в НКЦКИ отправлен. Если экспорт выполнен успешно, в НКЦКИ полученному инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**. При этом значение поля **Статус** меняется на *Отправлен в НКЦКИ*. С этого момента повторная отправка и редактирование инцидента в НКЦКИ в интерфейсе Kaspersky EDR Expert становятся недоступны. Если вам требуется внести изменения в экспортированный инцидент, это следует делать в личном кабинете НКЦКИ.

Допустимые категории и типы инцидентов НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ.

Категории и типы инцидентов НКЦКИ

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки
	Заражение вредоносным программным обеспечением (далее ВПО)
	Захват сетевого трафика
	Использование контролируемого ресурса для проведения атак
	Компрометация учетной записи
	Несанкционированное изменение информации
	Несанкционированное разглашение информации
	Публикация на ресурсе запрещенной законодательством РФ информации
	Успешная эксплуатация уязвимости
	Событие не связано с компьютерной атакой
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия

Статусы инцидента НКЦКИ

Инцидент, экспортированный в НКЦКИ, может иметь статусы, приведенные в таблице ниже.

Статусы инцидента НКЦКИ

Статус инцидента НКЦКИ	Описание
Черновик	Статус присваивается в следующих случаях: • экспорт инцидента не выполнялся; • экспорт инцидента был выполнен с ошибкой.
Отправлен в НКЦКИ	Статус присваивается в следующих случаях: • экспорт инцидента был выполнен успешно; • в НКЦКИ еще не был запрошен статус инцидента.
Создан	При успешном экспорте инциденту присваивается один из перечисленных статусов в зависимости от этапа рассмотрения инцидента специалистами НКЦКИ. Статус инцидента запрашивается в НКЦКИ каждые 5 минут после успешной отправки инцидента в НКЦКИ. После получения статуса *Принято решение* или *Отправлен в архив* запрос по инциденту в НКЦКИ больше не выполняется.
Создано	
Зарегистрирован	
Проверка НКЦКИ	
Принято решение	
Отправлен в архив	

Управление Sandbox

Sandbox – это компонент безопасности, который использует виртуальные машины (ВМ) с образами операционной системы для анализа поведения объектов, таких как файлы, приложения или скрипты, на предмет потенциальной вредоносной активности и признаков целевых атак на корпоративную ИТ-инфраструктуру.

Чтобы компонент Sandbox мог обрабатывать объекты, вам нужно настроить его, а затем установить на него виртуальные машины.

Первоначальная настройка Sandbox

Перед установкой виртуальных машин вам нужно настроить Sandbox:

- Настроить обновления баз данных.
- Убедиться, что доступ в интернет был правильно настроен во время установки Sandbox. При необходимости измените параметры.

Также вы можете изменить пароль администратора и настроить параметры политики аутентификации.

Настройка обновления баз для Sandbox

В течение срока действия лицензии Sandbox автоматически получает пакеты обновлений один раз в час.

Чтобы настроить обновления баз для Sandbox:

1. В веб-интерфейсе Sandbox перейдите в раздел **Обновление баз**.
2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать обновления:
   - **Серверы обновлений "Лаборатории Касперского"**

     Sandbox подключается к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и скачивает актуальные базы.
   - **Серверы обновлений "Лаборатории Касперского" (безопасное подключение)**

     Sandbox подключается к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS для скачивания актуальных баз. Рекомендуется выполнять безопасное обновление баз по протоколу HTTPS.
   - **Пользовательский сервер**

     Sandbox будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами приложения на вашем устройстве и загружать актуальные базы.

3. Если вы выбрали **Пользовательский сервер**:

   - Если вы хотите указать в качестве источника обновлений FTP- или HTTP-сервер, в поле под названием этого параметра укажите полный путь к папке с пакетом обновлений баз приложения для скачивания актуальных баз.

   - Если вы хотите указать в качестве источника обновлений сервер Kaspersky EDR Expert, на котором размещен компонент Sandbox, в поле под этим параметром укажите следующий адрес источника обновлений для скачивания актуальных баз:

     ```
     http://updater.<домен_smp>:8083/retranslation
     ```

4. Решите, использовать ли прокси-сервер при загрузке обновлений:

   - Чтобы включить прокси-сервер, включите переключатель рядом с названием группы параметров **Прокси-сервер**, а затем укажите параметры для подключения к прокси-серверу:

     - Адрес прокси-сервера и номер порта.

     - Имя пользователя и пароль прокси-сервера.

   - Чтобы выключить прокси-сервер, выключите переключатель рядом с названием группы параметров **Прокси-сервер**.

5. Нажмите на кнопку **Применить**, чтобы сохранить параметры.

Сетевые интерфейсы Sandbox

Настройка сетевых интерфейсов Sandbox включает в себя настройку DNS-серверов, настройку управляющих сетевых интерфейсов, управление доступом в интернет обрабатываемых объектов и добавление статических сетевых маршрутов.

Настройка параметров DNS

Чтобы настроить параметры DNS:

1. В веб-интерфейсе Sandbox перейдите в раздел **Сетевые интерфейсы**.

2. В поле **Имя устройства** укажите имя сервера для установки Sandbox. Имя сервера должно быть в формате FQDN.

3. Нажмите на кнопку **Добавить** справа от **DNS-серверы**.

4. В появившемся пустом поле введите IP-адрес главного DNS-сервера в формате IPv4.

5. Нажмите на кнопку ✓ справа от указанного IP-адреса.

DNS-сервер добавлен.

Чтобы добавить другие DNS-серверы, повторите шаги со 2 по 5.

Чтобы удалить ранее добавленный DNS-сервер, нажмите 🗑 справа от указанного IP-адреса DNS-сервера. Обратите внимание, что вы можете удалить только дополнительные DNS-серверы, но не главный DNS-сервер. Если вы добавили два и более DNS-серверов, вы можете удалить любой из них. Оставшийся DNS-сервер становится главным.

Настройка управляющего сетевого интерфейса

Управляющий сетевой интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH. Sandbox также получает объекты через этот интерфейс.

Управляющий сетевой интерфейс изначально настраивается во время установки компонента Sandbox. После установки Sandbox вы можете изменить параметры управляющего сетевого интерфейса с помощью веб-интерфейса Sandbox, как описано ниже.

Чтобы настроить управляющий сетевой интерфейс

1. В веб-интерфейсе Sandbox перейдите в раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. Настройте параметры управляющего интерфейса:
   - **IP**: IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
   - **Маска**: маска сети, в которой вы хотите использовать этот сетевой интерфейс.
4. Нажмите **Применить**.

Управляющий сетевой интерфейс настроен.

Настройка доступа в интернет для обрабатываемых объектов

Объекты, которые обрабатывает компонент Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Компонент Sandbox может анализировать поведение этих объектов. Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

Риски и соображения безопасности

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и сетевой интерфейс Sandbox для доступа в интернет открыт, есть риск возникновения следующего сценария:

1. Злоумышленник может прикрепить вредоносное приложение к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети.
2. Этот файл будет выведен за пределы локальной сети в процессе проверки файла.

Если доступ в интернет для обрабатываемого объекта заблокирован, этот риск исключен. Однако это также означает снижение качества алертов, поскольку обработанные объекты не могут быть должным образом проанализированы.

Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет:

1. В веб-интерфейсе Sandbox перейдите в раздел **Сетевые интерфейсы**.
2. В группе параметров **Интерфейс для выхода в интернет** в списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.
3. Настройте параметры интерфейса:
   - **IP**: IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
   - **Маска**: маска сети, в которой вы хотите использовать этот сетевой интерфейс.
   - **Шлюз по умолчанию**: адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
4. Нажмите **Применить**.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет настроен.

Добавление статического сетевого маршрута

Чтобы добавить статический сетевой маршрут:

1. В веб-интерфейсе Sandbox перейдите в раздел **Сетевые интерфейсы**.
2. В группе параметров **Static routes** нажмите на кнопку **Add**.
   В списке статических сетевых маршрутов появится набор пустых полей.
3. Настройте параметры маршрута:
   - **IP**: IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
   - **Маска**: маска подсети.
   - **Шлюз соединения**: IP-адрес шлюза соединения.
4. В списке **Interface** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
5. Нажмите на кнопку ✓ справа от указанного маршрута.
6. Нажмите на кнопку **Применить**.

Статический сетевой маршрут добавлен.

После добавления статического сетевого маршрута вы можете управлять маршрутом, нажав на кнопку 🗑 или ✎, чтобы удалить или изменить его. При изменении маршрута вам нужно будет указать те же параметры, как и при создании маршрута, описанные выше.

Изменение пароля учетной записи администратора Sandbox

Чтобы изменить пароль учетной записи администратора Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование** → **Изменить пароль**.
2. В поле **Текущий пароль** введите текущий пароль, который вы использовали для входа в Sandbox.
3. В полях **Новый пароль** и **Подтверждение пароля** введите новый пароль.
4. Нажмите на кнопку **Изменить пароль**.

Политики аутентификации в Sandbox

Для пользователей Kaspersky EDR Expert можно настроить политики аутентификации в Sandbox.

Завершение неактивных сессий

Если пользователь не выполняет никаких действий (сеанс неактивен), рекомендуется завершать такой сеанс. Это снижает риск несанкционированного доступа к Sandbox, когда пользователь фактически закончил работу с приложением, но его сеанс остался незавершенным.

Информирование о неуспешных попытках аутентификации

Частые неудачные попытки входа в веб-интерфейс могут быть признаком того, что к Sandbox пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Завершение неактивных сеансов в Sandbox

Если пользователь не выполняет никаких действий (сеанс неактивен), рекомендуется завершать такой сеанс. Это снижает риск несанкционированного доступа к Sandbox, когда пользователь фактически закончил работу с приложением, но его сеанс остался незавершенным.

Чтобы включить и настроить завершение неактивных сессий:

1. В веб-интерфейсе Sandbox перейдите в раздел **Политики аутентификации**.

2. В разделе **Завершение неактивных сеансов** укажите время, по истечении которого пользовательский сеанс должен быть завершен, если пользователь не выполняет никаких действий. Время в минутах введите в поле **Завершить неактивные сеансы после**.

3. Нажмите **Применить**.

Sandbox завершает неактивные пользовательские сеансы по истечении указанного времени.

Информирование о неуспешных попытках аутентификации на Sandbox

Частые неудачные попытки входа в веб-интерфейс могут быть признаком того, что к Sandbox пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Чтобы включить и настроить информирование о неуспешных попытках аутентификации:

1. В веб-интерфейсе Sandbox перейдите в раздел **Политики аутентификации**.

2. В разделе **Количество попыток аутентификации** переместите переключатель **Количество попыток** в положение **Включено**.

3. В поле **Период подсчета** введите время, в течение которого должны подсчитываться неуспешные попытки аутентификации. Время указывается в минутах. Если в течение этого времени пользователь неуспешно пытается войти в веб-интерфейс или консоль управления более двух раз подряд, происходит следующее:

   - В журнал активности пользователей вносится запись о неуспешных попытках аутентификации пользователя.

   - Если было создано правило для отправки уведомлений о превышении количества неудачных попыток аутентификации, отправляется сообщение электронной почты на адреса, указанные в правиле уведомления. В сообщении содержится информация о неуспешных попытках аутентификации пользователя.

   В поле **Период подсчета** допускается указать `0`, в этом случае подсчитываются все неуспешные попытки аутентификации, вне зависимости от временного интервала между ними.

4. Нажмите **Применить**.

Подготовка виртуальных машин к работе

Sandbox использует виртуальные машины для запуска объектов в различных операционных системах с целью анализа поведения объектов и обнаружения их вредоносной активности.

Вы можете устанавливать виртуальные машины двух типов:

- *Преднастроенные* или *по умолчанию*. Это виртуальные машины на основе образов операционных систем (файлы с расширением ISO) из дистрибутива. Эти образы или установленные на них приложения недоступны для изменения.

  > Вам потребуется активировать некоторые операционные системы и приложения. Активация производится с помощью ваших лицензий.

- *Пользовательские*. Это виртуальные машины на основе выбранных вами операционных систем. На эти операционные системы можно устанавливать любые приложения.

Вы можете использовать пользовательские и преднастроенные образы операционных систем одновременно.

Установка виртуальных машин включает следующие шаги:

1. *Необязательно*. Загрузка образов в Хранилище. Вы можете пропустить этот шаг и загрузить образы со своего устройства при создании шаблона.

2. Создание шаблона с помощью импорта преднастроенного шаблона или создания пользовательского шаблона виртуальной машины.

3. *Для пользовательских шаблонов*. Настройка операционной системы и программного обеспечения.

4. Создание виртуальной машины.

5. Установка виртуальной машины.

Загрузка образов в Хранилище

Чтобы загрузить образ в Хранилище:

1. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Хранилище**.

2. Нажмите на кнопку **Загрузить**.

3. Выберите файл с расширением .ISO, который вы хотите загрузить в Хранилище и нажмите **Открыть**.

Импорт шаблона

Импорт шаблона – это первый шаг, если вы хотите установить преднастроенную виртуальную машину.

Вы также можете импортировать шаблон пользовательской виртуальной машины, если вы создали и экспортировали его ранее.

Чтобы импортировать шаблон виртуальной машины:

1. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Шаблоны**.
2. В раскрывающемся списке **Добавить** выберите **Импортировать шаблон**.
3. Выберите файл для импорта и нажмите **Открыть**.

Создание пользовательского шаблона виртуальной машины

Чтобы создать пользовательский шаблон виртуальной машины:

1. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Шаблоны**.
2. В раскрывающемся списке **Добавить** выберите **Создать шаблон**.

   Откроется окно создания шаблона.
3. На шаге **Подготовка образа**:
   a. Укажите **Имя** и **Описание**.
   b. Чтобы указать операционную систему для шаблона, выполните одно из следующих действий:
      - Выберите образ из списка доступных образов в раскрывающемся списке **Образы ОС**.
      - Загрузите образ операционной системы: нажмите **Загрузить**, выберите ISO-файл и нажмите **Открыть**.
   c. Нажмите на кнопку **Продолжить**.
4. На шаге **Настройка шаблона**:
   a. В раскрывающемся списке **Смонтировать ISO** выберите образ приложения, которое вы хотите установить в операционной системе.

      Чтобы образ отображался в списке, вам нужно выполнить одно из следующих действий:
      - Загрузить образ в Хранилище.
      - Загрузите файл образа приложения: нажмите **Загрузить**, выберите ISO-файл и нажмите **Открыть**.
   b. После установки приложения размонтируйте установленный образ: в раскрывающемся списке **Монтировать ISO** нажмите на значок ⏏ рядом с образом.
   c. Настройте операционную систему и программное обеспечение, установленное в ней.

Настройка операционной системы и программного обеспечения

Подготовка операционных систем к работе

При установке операционных систем Windows 7, 8.1 или 10 выполните следующие требования:

- Отключите экранную заставку.
- Выберите схему питания Всегда включено.
- Отключите автоматическое обновление.
- Отключите сетевой экран Windows.

При использовании операционной системы Windows 7 требуется поддержка хеш-алгоритма SHA-2. Для поддержки этого хеш-алгоритма установите обновление Security Update for Windows 7 for x64-based Systems (KB3033929). Для 32-разрядных операционных систем Windows 7 также требуется установить обновление KB3033929.

> Не устанавливайте обновление KB4474419. Это обновление может вызвать сбой во время развертывания виртуальной машины.

Для использования Windows 7 необходимо в настройках операционной системы включить использование TLS 1.1 и TLS 1.2. Для этого в Windows 7 в разделе **Панель управления** → **Свойства браузера** → **Дополнительно** установите флажок **Использовать TLS 1.1** и **Использовать TLS 1.2**.

При использовании операционных систем Windows 8.1 и 10 требуется отключить быструю загрузку и включить автоматический вход в систему.

Локализация операционных систем

Вы можете выбрать язык локализации при установке системы или установить систему с английской локализацией и дополнительно установить пакет локализации в эту систему. Вы можете выбрать один из следующих языков: русский, английский, китайский (упрощенный), арабский, испанский (Мексика). При выборе другой локализации качество проверки объектов будет снижено.

> Для операционной системы Windows XP поддерживаются только русский и английский языки.

Настройка операционных систем

С установленной операционной системой требуется выполнить следующие действия:

- Убедиться, что включено использование командной оболочки по умолчанию.
- Активировать операционную систему и другое лицензионное программное обеспечение.

Вы можете выполнить с установленной операционной системой следующие действия:

- Присвоить статичное имя компьютеру.
- Создать учетные записи пользователей.

  В этом случае требуется настроить автоматический вход в систему.

- Установить программное обеспечение.

  Ограничения, действующие при установке программного обеспечения:

  - К одному шаблону единовременно можно подключить только один образ. После того как шаблон будет сохранен, вы можете отключить один образ и подключить другой.
  - Не поддерживаются версии Microsoft Office выше 2016.
  - Настоятельно не рекомендуется устанавливать программное обеспечение следующих типов:
    - Программное обеспечение, внедряющее свой код в другой запущенный процесс.
    - Драйверы для защиты.
    - Антивирусные приложения, включая Защитник Windows.
  - Не гарантируется обнаружение вредоносной активности файлов, которые запускаются с помощью узкоспециального программного обеспечения.

Kaspersky EDR Expert не уведомляет о проблемах с установленным в операционной системе программным обеспечением.

Создание виртуальной машины

Чтобы создать виртуальную машину с пользовательским образом операционной системы, требуется соединение с интернетом.

Чтобы создать виртуальную машину:

1. *Для пользовательских шаблонов*. Убедитесь, что шаблон, используемый для создания виртуальной машины, отключен от питания.

   a. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Шаблоны**.

   b. Выберите шаблон.

   c. Если шаблон включен, выберите один из вариантов в раскрывающемся списке **Выключить**:

      - **Выключить**, если вы хотите завершить работу системы с сохранением результата работы запущенных приложений.

      - **Выключить питание**, если вы хотите завершить работу системы без сохранения результатов работы.

2. В веб-интерфейсе Sandbox перейдите в раздел **Виртуальные машины**.

3. Нажмите на кнопку **Создать VM**.

4. В раскрывающемся списке **Шаблон** выберите интересующий вас шаблон.

5. *Для пользовательских операционных систем*: укажите **имя** виртуальной машины и **описание**.

6. Нажмите на кнопку **Сохранить**.

7. *Для преднастроенных операционных систем*: некоторые операционные системы из дистрибутива требуют принятия условий Лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

8. *Для пользовательских операционных систем*: если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы.

Установка виртуальной машины

Чтобы установить виртуальную машину с преднастроенной операционной системой:

1. В веб-интерфейсе Sandbox перейдите в раздел **Виртуальные машины** → **Преднастроенные**.

2. В разделе **Неустановленные виртуальные машины** нажмите на кнопку **Установить готовые VM**.

Чтобы установить виртуальную машину с пользовательской операционной системой:

1. В веб-интерфейсе Sandbox перейдите в раздел **Виртуальные машины** → **Пользовательские**.

2. Найдите нужную виртуальную машину и в столбце **Действия** перейдите по ссылке **Установить**.

3. Когда виртуальная машина установится, в столбце **Действия** перейдите по ссылке **Включить**.

Загрузка отладочных символов

Если для сервера, на котором устанавливается виртуальная машина с пользовательским образом, не настроен доступ в интернет, для корректного завершения установки виртуальной машины вам нужно загрузить отладочные символы Microsoft.

> Для корректной загрузки отладочных символов в операционной системе, которая используется для шаблона виртуальной машины, должны быть установлены средства для отладки Windows (Windows Debug Tools) и имя устройства, подключенного к сети (hostname), должно содержать только латинские буквы, цифры и специальные символы.

Чтобы скачать отладочные символы:

1. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Шаблоны**.
2. Выберите шаблон.
3. В окне с ошибкой **Нет доступа в интернет** нажмите на кнопку **Скачать манифест**.

   > Кнопка **Скачать манифест** не будет доступна, пока виртуальная машина не получит статус **Сбой**.

4. Распакуйте скачанный архив.
5. Запустите файл sbsymtool.ps1 с помощью Windows PowerShell.

   Архив с отладочными символами будет загружен в папку с этим файлом.
6. В веб-интерфейсе Sandbox перейдите в раздел **Шаблоны и Хранилище** → **Шаблоны**.
7. Выберите шаблон, для которого вы загрузили отладочные символы.
8. В раскрывающемся списке **Действия** выберите **Загрузить символы**.
9. В открывшемся окне выберите архив с отладочными символами и нажмите на кнопку **Открыть**.

Отладочные символы будут загружены.

Настройка OSMP для использования технологий обнаружения

Kaspersky EDR Expert обнаруживает угрозы с помощью различных технологий обнаружения, таких как Anti-Malware Engine или Sandbox. Вам нужно настроить OSMP, чтобы использовать технологии обнаружения.

Anti-Malware Engine

Для Anti-Malware Engine выполните следующие действия:

- Настройте получение обновлений антивирусных баз.
- Создайте список паролей для архивов, защищенных паролем.

Sandbox

После того как вы установили и настроили Sandbox и установили виртуальные машины в Sandbox, вам нужно сделать следующее:

- Настройте получение обновлений антивирусных баз.
- Выберите операционные системы для проверки объектов.
- Создайте пользовательские правила Sandbox, если вы собираетесь использовать пользовательские операционные системы.
- Настройте отправку файлов от Endpoint Agent.

YARA

Для YARA-проверки выполните следующие действия:

Импорт YARA-правил

IOC

Для IOC-проверки выполните следующие действия:

- Настройка IOC-проверки по расписанию
- Импорт IOC-правил

Обновление антивирусных баз Sandbox и Anti-Malware Engine

При проверке объектов Sandbox и Anti-Malware Engine и требуется наличия актуальных антивирусных баз, поэтому антивирусные базы должны обновляться регулярно. В качестве источника обновлений вы можете использовать один из серверов "Лаборатории Касперского" или собственный источник, которым может быть HTTP-сервер, FTP-сервер или папка.

Kaspersky EDR Expert автоматически ищет новые пакеты обновлений в указанном источнике каждые 30 минут. Также вы можете в любое время обновить антивирусные базы вручную.

Чтобы настроить получение обновлений для Sandbox и Anti-Malware Engine, у вас должна быть одна из следующих ролей EDR: Главный администратор, Администратор SOC, Администратор тенанта, Аудитор. Пользователи с ролью Аудитор могут просматривать только текущий источник обновлений. Пользователи с другими ролями могут просматривать и менять источник обновлений.

Чтобы настроить получение обновлений для Sandbox и Anti-Malware Engine:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на **корневой** тенант (параметры обновления для других тенантов недоступны для изменения).

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры**.

4. В разделе **Проверяется** выберите вкладку **Обновление баз**.

5. В раскрывающемся списке **Источник обновлений** выберите один из источников обновлений:

   - **Серверы обновлений "Лаборатории Касперского" (безопасное подключение)**

     Kaspersky EDR Expert будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется скачать обновление баз по протоколу HTTPS.

   - **Серверы обновлений "Лаборатории Касперского"**

     Kaspersky EDR Expert будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

- **Пользовательский сервер**

  Kaspersky EDR Expert подключается к вашему источнику обновлений, чтобы скачать актуальные базы. Укажите путь к источнику обновлений в **URL или путь к папке**. Это может быть URL, HTTP-сервер или FTP-сервер, а также полный путь к папке, содержащей пакет обновлений.

6. Если вы хотите обновить антивирусные базы сейчас, нажмите на кнопку **Обновление**.

7. Нажмите на кнопку **Сохранить**.

Получение обновлений для Sandbox и Anti-Malware Engine настроено. Kaspersky EDR Expert отображает информацию о последнем обновлении в поле **Обновлено**.

Вы можете в любое время обновить антивирусные базы вручную, нажав на кнопку **Обновление**.

Создание списка паролей для архивов, защищенных паролем

По умолчанию Kaspersky EDR Expert не может выполнять проверку объектов в архивах, защищенных паролем. Такие архивы необходимо сначала распаковать. Вы можете создать список паролей, которые обычно используются для архивов в вашей организации. Kaspersky EDR Expert использует пароли из списка при проверке архива. Если один из паролей подходит, Kaspersky EDR Expert распаковывает архив и выполняет проверку находящихся в нем объектов.

Для работы со списком паролей для архивов, защищенных паролем, у вас должна быть одна из следующих ролей EDR: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня, Аудитор.
Пользователи с ролью Аудитор могут только просматривать список паролей. Пользователи с другими ролями могут просматривать список и вносить в него изменения.

Чтобы сформировать список паролей для распаковки архивов, защищенных паролем:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на **корневой** тенант (список паролей для других тенантов недоступен для изменения).

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры**.

4. В разделе **Проверяется** выберите вкладку **Архивы**.

5. В поле **Пароль для архивов** добавьте пароли для распаковки архивов, защищенных паролем, каждый пароль в новой строке.

6. Если вы хотите ограничить доступ к списку паролей, включите переключатель **Для доступа к списку паролей требуется пароль**, а затем укажите пароль в панели **Установка пароля доступа**. Вы можете поделиться этим паролем с пользователями OSMP, которым требуется доступ к списку паролей для архивов, защищенных паролем.

   Нажмите на кнопку **Сохранить**, чтобы сохранить пароль доступа.

При необходимости вы можете изменить этот пароль позже, нажав на кнопку **Изменение пароля** на вкладке **Архивы**.

7. Нажмите на кнопку **Сохранить** или **Сохранить и закрыть**, чтобы сохранить список паролей для архивов, защищенных паролем.

Выбор операционных систем для проверки объектов в Sandbox

Компонент Sandbox запускает объекты в нескольких операционных системах и анализирует их поведение для обнаружения вредоносной активности и индикаторов целевых атак и вторжений в корпоративную ИТ-инфраструктуру.

Вы можете выбрать операционные системы для проверки объектов. Это может быть один из преднастроенных наборов, пользовательский набор или их комбинация.

Чтобы выбрать набор операционных систем:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры**.

4. В разделе **Серверы Sandbox** перейдите по ссылке рядом с полем **Операционные системы для проверки**.

5. В открывшейся панели **Изменение набор операционных систем** в разделе **Набор операционных систем** выберите один из стандартных наборов операционных систем или **Пользовательская**.

   Если вы хотите объединить преднастроенные операционные системы с другими операционными системами, выберите **Пользовательская**.

6. Если вы выбрали **Пользовательская**, список доступных операционных систем отображается в разделе **Содержимое набора**.

   В этот список всегда входят преднастроенные операционные системы. Если в Sandbox нет виртуальной машины с преднастроенной операционной системой, эта операционная система имеет статус **Неизвестно**.

   Список включает пользовательскую операционную систему, если на сервере Sandbox есть виртуальная машина, на которой работает эта операционная система.

   Установите флажки рядом с операционными системами, которые вы хотите включить в набор.

7. Нажмите на кнопку **Сохранить**.

Набор операционных систем для проверки объектов готов.

Для пользовательского набора операционных систем вам также нужно создать пользовательские правила.

Создание пользовательских правил Sandbox

Если вы выбрали пользовательские операционные системы для проверки объектов, вам также нужно создать пользовательские правила, которые определяют, какие объекты следует проверять и в какой операционной системе.

Вам не нужно создавать правила отправки объектов на проверку в преднастроенные операционные системы, Kaspersky EDR Expert отправляет объекты туда автоматически.

> Пользовательские правила Sandbox применяются только к пользовательским виртуальным машинам, созданным в веб-интерфейсе Sandbox.

Чтобы добавить пользовательское правило Sandbox:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила Sandbox**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно создания правила.
3. Настройте следующие параметры:
   - Включите переключатель **Статус правила**, если вы хотите включить правило сразу после его создания.
   - Выберите владельца тенанта.
   - Выберите виртуальную машину, на которой нужно выполнять проверку файлов.

     Вы можете выбирать только виртуальные машины, с выбранными вами пользовательским операционными системами.
   - В блоке **Критерии соответствия** выберите, хотите ли вы использовать критерии **Маска**, **Категория файла** или **Оба** в качестве критерия сопоставления.
   - Если вы выбрали **Маска** или **Оба** в качестве критерия соответствия:
     - Укажите значение для поля **Маска** для имен файлов, которые будут отправлены в Sandbox в соответствии с правилом.

       Вы можете указать несколько значений, каждое в отдельной строке.

       Вы можете использовать символы подстановки * и ?. Другие символы подстановки не поддерживаются.
     - Укажите необязательную значение **Маска исключений** для файлов, которые должны быть исключены из проверки, даже если их имена соответствуют указанной ранее маске.

       Вы можете указать несколько значений, каждое в отдельной строке.

       Вы можете использовать символы подстановки * и ?. Другие символы подстановки не поддерживаются.

Вы можете использовать поле **Маска исключений**, если только на виртуальных машинах, отмеченных в списке **Серверы Sandbox** для параметров **Пользовательский набор** выбран параметр **Пользовательская**. Если выбраны и другая виртуальная машина и предварительно настроенная виртуальная машина, поле **Маска исключений** игнорируется.

- Если вы выбрали **Категория файла** или **Оба** в качестве критерия соответствия:

  В раскрывающемся списке **Категория файла** выберите категории файлов, которые будут отправлены в Sandbox в соответствии с правилом.

- Чтобы ограничить размер файлов, отправляемых в Sandbox, нажмите на кнопку **Добавить размер файла**, а затем укажите значения **Минимальный** и **Максимальный** для размера файла. Таким образом, вы можете установить несколько диапазонов размеров.

4. Нажмите на кнопку **Сохранить**.

Правило отобразится в списке пользовательских правил Sandbox.

Особенности проверки архивов

Проверка архивов выполняется следующим образом:

1. Kaspersky EDR Expert распаковывает архив.
2. Если какие-то файлы из архива соответствуют правилу, Kaspersky EDR Expert отправляет их на проверку.

Файлы с расширением MSI обрабатываются аналогично архивам.

Настройка отправки файлов от Endpoint Agent в Sandbox

Endpoint Agent могут отправлять файлы в Sandbox для проверки несколькими способами:

- Endpoint Agent **автоматически** обнаруживает объекты и отправляет их в Sandbox для проверки.
- Пользователь Endpoint Agent **вручную** передает файл на проверку.
- Endpoint Agent отправляет файл, который запустил **IOA-правило**. Если на устройстве срабатывает IOA-правило и это IOA-правило содержит условие для отправки обнаруженных объектов в Sandbox, Kaspersky EDR Expert автоматически инициирует действие по реагированию **Получить файл** с включенным параметром **Проверить файл**.

Автоматическая отправка файлов в Sandbox может значительно увеличить нагрузку на OSMP.

Чтобы настроить отправку файлов для проверки в Sandbox:

1. Убедитесь, что настроена интеграция Sandbox с OSMP.

2. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

3. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

4. Выберите вкладку **Параметры**.

5. В разделе **Проверяется** выберите вкладку **Sandbox**.

6. Настройте параметры:

   - Чтобы включить **автоматическую** отправку файлов, обнаруженных Endpoint Agent:

     В блоке **Отправлять файлы с устройств для анализа в Sandbox** включите переключатель **Отправлять файлы автоматически**.

     По умолчанию параметр выключен.

   - Чтобы включить отправку файлов пользователем **вручную**:

     В блоке **Отправлять файлы с устройств для анализа в Sandbox** включите переключатель **Отправлять файлы вручную**.

     По умолчанию эта функция включена.

   - Чтобы включить отправку файлов при срабатывании **IOA-правила**:

     В блоке **Автоматически отправлять файлы в Sandbox** включите переключатель **Отправить файлы**.

     По умолчанию параметр выключен.

7. Нажмите на кнопку **Сохранить и закрыть**.

Отправка файлов в Sandbox настроена. По результатам проверки Kaspersky EDR Expert может создать алерт.

Об индикаторах компрометации, IOC-файлах и IOC-правилах

Kaspersky EDR Expert может выполнять проверку устройств на наличие индикаторов компрометации. Индикаторы компрометации (IOC) – это цифровые объекты, такие как хеши файлов или IP-адреса, которые могут предупреждать о кибератаке. Вы можете узнать больше о IOC на веб-сайте ИТ-энциклопедия "Лаборатории Касперского" и Securelist.

IOC-файлы

Несколько IOC можно объединить в структурированное описание в *IOC-файле*. Для таких файлов существует стандартный *формат OpenIOC*.

Ниже приведен пример простого IOC-файла.

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="unique
ID in the UUID format" last-modified="date of the last modification of the rule in the YYYY-MM-DDThh:mm:ss format"
xmlns="http://schemas.mandiant.com/2010/ioc">
        <short_description>Rule name</short_description>
        <authored_by>Rule name</authored_by>
        <authored_date>file creation date in the YYYY-MM-DDThh:mm:ss format</authored_date>
        <links />
        <definition>
                <Indicator operator="OR" id="Unique ID in the UUID format">
                        <IndicatorItem id="Unique ID in the UUID format" condition="is">
                                <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
                                <Content type="md5">MD5 hash of the file</Content>
                        </IndicatorItem>
                </Indicator>
        </definition>
</ioc>
```

Вы можете создать свой IOC-файл в текстовом редакторе и сохранить его с расширением .ioc. В зависимости от приложения Endpoint Agent вы можете использовать термины OpenIOC, перечисленные в файлах:

Условия OpenIOC для Kaspersky Endpoint Security для Windows

Условия OpenIOC для Kaspersky Endpoint Security для Linux

Нет списка условий OpenIOC для Kaspersky Endpoint Security для Mac, поскольку Kaspersky EDR Expert не отправляет задачи IOC-проверки в Kaspersky Endpoint Security для Mac.

IOC-правила

При импорте IOC-правила Kaspersky EDR Expert извлекает структурированное описание из IOC-файла и создает правило на основе описания.

IOC-правила доступны в списке IOC-правил в интерфейсе Консоли OSMP → **Мониторинг** → **Ресурсы и сервисы** → **IOC-правила**.

Настройка IOC-проверки по расписанию

Для IOC-проверки на устройствах с установленным компонентом Endpoint Agent можно настроить расписание. Если задано расписание, Endpoint Agent ежедневно выполняют поиск индикаторов компрометации на устройствах в соответствии с IOC-правилами, для которых включен запуск проверки по расписанию.

По умолчанию IOC-проверка выполняется ежедневно. Вы можете изменить время начала и продолжительность проверки или выключить ежедневную проверку.

Для настройки IOC-проверки по расписанию выполните действия в следующем порядке:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры**.

4. В разделе **Параметры сканирования** выберите вкладку **Расписание IOC-проверки**.

5. Включите переключатель **Ежедневная проверка** и задайте параметры расписания проверки:

   - **Время начала (UTC)**. Время начала IOC-проверки. Время указывается в часовом поясе сервера OSMP, на котором выполняется настройка.

     Если приложение Endpoint Agent получает новое расписание проверки позже времени, указанного в поле **Время начала (UTC)**, следующая проверка запускается на следующий день в момент времени, указанный в поле **Время начала (UTC)**.

   - **Максимальная продолжительность проверки (в часах)**. Ограничение по времени для IOC-проверки в часах. По истечении этого времени приложение Endpoint Agent завершает процесс проверки независимо от его завершенности.

6. Нажмите на кнопку **Сохранить** или **Сохранить и закрыть**, чтобы сохранить параметры.

Новое расписание IOC-проверки становится активно сразу после сохранения изменений. Если при сканировании будет обнаружена угроза, будет создан IOC-алерт.

Ограничения для Kaspersky Endpoint Security для Windows

Если область поиска IOC, определенная в IOC-правиле, включает тип данных RegistryItem, Kaspersky Endpoint Security для Windows проверяет ограниченный набор ключей реестра.

Импорт IOC-правил

Kaspersky EDR Expert импортирует IOC-правила из файла, содержащего IOC-правила. Один файл может содержать только одно IOC-правило, поэтому список IOC-правил также является списком файлов IOC, из которых были созданы правила.

Список IOC-правил доступен в интерфейсе Консоли OSMP → **Мониторинг** → **Ресурсы и сервисы** → **IOC-правила**.

Чтобы импортировать IOC-правило:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **IOC-правила**.

   Откроется список IOC-правил.

2. Нажмите на кнопку **Импортировать**.

3. В открывшейся панели **Импорт IOC-правил** настройте следующие параметры:

   - В раскрывающемся списке **Тенант** выберите тенант.

   - В раскрывающемся списке **Важность** выберите уровень важности правила. Kaspersky EDR Expert присваивает это значение алерту, создаваемому в результате срабатывания IOC-правила.

   - Если вы хотите, чтобы приложение Kaspersky EDR Expert регулярно выполняло проверку устройств на наличие индикаторов компрометации, описанных в правиле, включите переключатель **Проверка по расписанию** (расписание проверки должно быть настроено).

     Вы также можете включить проверку по расписанию позже, включив переключатель в столбце **Проверка по расписанию** в списке правил IOC.

4. Загрузите файл, содержащий IOC-правило.

5. Нажмите на кнопку **Импортировать**.

Импортированное правило отобразится в списке IOC-правил.

Импорт YARA-правил

Kaspersky EDR Expert использует YARA-правила для проверки файлов, отправляемых в OSMP, и для проверки устройств.

Kaspersky EDR Expert импортирует YARA-правила из файла, содержащего YARA-правила. Один файл может содержать несколько YARA-правил. Kaspersky EDR Expert анализирует файл, извлекает правила и добавляет их в список правил. Импорт файла, содержащего более 65 535 правил, не гарантируется.

Список YARA-правил доступен в интерфейсе Консоли OSMP → **Мониторинг** → **Ресурсы и сервисы** → **YARA-правила**.

Чтобы импортировать YARA-правила:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **YARA-правила**.

   Откроется список YARA-правил.

2. Нажмите на кнопку **Импортировать**.

3. В открывшейся панели **Импорт YARA-правил** настройте следующие параметры:

   - В раскрывающемся списке **Тенант** выберите нужный тенант.

   - Для уровня важности любого YARA-правила по умолчанию задано значение **Высокий** и это значение невозможно изменить. Kaspersky EDR Expert присваивает это значение алерту, создаваемому в результате срабатывания YARA-правила.

   - Если вы хотите, чтобы приложение Kaspersky EDR Expert использовало все импортированные правила для проверки файлов, отправляемых в OSMP, включите переключатель **Проверка файла**.

     Вы также можете включить любое правило в список YARA-правил для проверки файлов позже, включив переключатель в столбце **Проверка файла** списка YARA-правил.

Эта функция доступна только для корневого тенанта.

- Укажите описание (необязательно).

4. Загрузите файл с YARA-правилами.

   При загрузке файла Kaspersky EDR Expert извлекает правила из файла и отображает информацию об извлеченных правилах.

5. Нажмите на кнопку **Импортировать**.

Импортированные правила отобразятся в списке YARA-правил.

Работа с Open Single Management Platform

Open Single Management Platform (далее OSMP) – это технологическая платформа, которая позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности и обеспечивает кросс-программные сценарии.Для управления Kaspersky EDR Expert OSMP используется веб-интерфейс (далее Консоль OSMP).

С помощью Консоли OSMP вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- просматривать информацию о безопасности сети вашей организации;
- настраивать обнаружения, поиск и реагирование на угрозы;
- управлять политиками, сформированными для активов вашей сети;
- управлять задачами приложений, установленных на устройствах сети;
- управлять пользователями и ролями;
- настраивать перенос данных в Kaspersky EDR Expert;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями;
- опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически;
- управлять интеграцией Kaspersky EDR Expert с другими приложениями.

Консоль OSMP – это мультиязычный веб-интерфейс. Вы можете изменить язык интерфейса в любое время без повторного открытия приложения.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования.

Настройка адреса подключения Сервера администрирования

Адрес подключения к Серверу администрирования – это сетевой адрес, который используется для следующих целей:

- Как адрес по умолчанию при создании инсталляционных пакетов Агента администрирования.

  После установки Агента администрирования управляемые устройства подключаются к Серверу администрирования по этому адресу.

- Как адрес прокси-сервера KSN.

  Управляемые устройства подключаются к прокси-серверу KSN с по этому адресу.

Чтобы настроить адрес подключения Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.

3. В открывшемся окне в поле **Адрес подключения Сервера администрирования** укажите новый адрес подключения Сервера администрирования.

   Максимальная длина адреса подключения составляет 255 символов.

   Вы можете указать адрес подключения к Серверу администрирования как NetBIOS-имя, FQDN или IP-адрес Сервера администрирования.

4. Нажмите на кнопку **Сохранить**.

Указанный адрес используется в качестве адреса Сервера администрирования и адреса прокси-сервера KSN.

Настройка параметров подключения OSMP Console к Серверу администрирования

Вы можете настроить подключение OSMP Console к Серверу администрирования через свойства Сервера администрирования или с помощью параметров политики Сервера администрирования.

Чтобы задать порты подключения с помощью свойств Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

Основные параметры подключения выбранного Сервера указаны.

Чтобы задать порты подключения с помощью свойств политики Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Нажмите на название политики Сервера администрирования и перейдите на вкладку **Параметры приложения**.

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

> Если вы выключите параметр **Открыть порт для Kaspersky Security Center Web Console** и этот параметр политики будет применен к устройству, вы не сможете подключиться к Серверу администрирования с помощью OSMP Console. В этом случае соединение будет прервано. Если у вас есть Сервер администрирования, на котором не применяется эта политика, вы можете повторно подключиться к этому Серверу администрирования с помощью OSMP Console.

Основные параметры подключения выбранного Сервера указаны.

Настройка параметров доступа к интернету

Подключение к интернету необходимо для правильной работы компонентов Kaspersky EDR Expert и может использоваться для определенных интеграций как с "Лабораторией Касперского", так и со сторонними производителями. Например, доступ для Сервера администрирования к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky EDR Expert и управляемых приложений "Лаборатории Касперского".

В параметрах интеграции некоторых программ "Лаборатории Касперского" есть возможность включить или выключить использование прокси-сервера. Например, такая возможность доступна при настройке интеграции с Kaspersky Threat Intelligence Portal.

Чтобы указать параметры доступа к интернету:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры доступа к сети интернет**.

3. Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Kaspersky EDR Expert к интернету.

   - **Номер порта**

     Номер порта, через который будет установлено прокси-подключение Kaspersky EDR Expert.

   - **Не использовать прокси-сервер для локальных адресов**

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - **Аутентификация на прокси-сервере**

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

     Поле ввода доступно, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя**

  Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

- **Пароль**

  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Сертификаты для работы с Open Single Management Platform

В этом разделе содержится информация о сертификатах Open Single Management Platform и описание, как выпустить и заменить сертификаты для OSMP Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с OSMP Console.

О сертификатах Open Single Management Platform

Open Single Management Platform использует следующие типы сертификатов для обеспечения безопасного взаимодействия между компонентами приложения:

- сертификат Сервера администрирования;
- сертификат Сервера Консоли OSMP;
- сертификат Консоли OSMP.

По умолчанию Open Single Management Platform использует самоподписанные сертификаты (то есть выданные самим Open Single Management Platform). Если требуется, вы можете заменить самоподписанные сертификаты пользовательскими сертификатами, в соответствии со стандартами безопасности вашей организации. После того как Сервер администрирования проверит соответствие пользовательского сертификата всем применимым требованиям, этот сертификат приобретает такую же область действия, что и самоподписанный сертификат. Единственное отличие состоит в том, что пользовательский сертификат не перевыпускается автоматически по истечении срока действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert или в Консоли OSMP в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

- C – общий сертификат для портов 13000 и 13291;
- CR – общий резервный сертификат для портов 13000 и 13291.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для следующих целей:

- Аутентификация Сервера администрирования при подключении к Консоли OSMP.
- Безопасное взаимодействие Сервера администрирования и Агента администрирования на управляемых устройствах.
- Аутентификация при подключении главных Серверов администрирования к подчиненным Серверам администрирования.

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке /var/opt/kaspersky/klnagent_srv/1093/cert/. Сертификат Сервера администрирования вы указываете при создании файла ответов для установки Консоли OSMP. Этот сертификат называется общим ("C").

Сертификат Сервера администрирования действителен 397 дней. Open Single Management Platform автоматически создает общий резервный сертификат ("CR") за 90 дней до истечения срока действия общего сертификата. Общий резервный сертификат впоследствии используется для замены сертификата Сервера администрирования. Когда истекает срок действия общего сертификата, общий резервный сертификат используется для поддержания связи с экземплярами Агента администрирования, установленными на управляемых устройствах. С этой целью общий резервный сертификат автоматически становится новым общим сертификатом за 24 часа до истечения срока действия старого общего сертификата.

> Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

При необходимости можно назначить Серверу администрирования пользовательский сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата. При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "*Ошибка аутентификации Сервера администрирования*". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата.

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных.

Вы также можете создать резервную копию сертификата Сервера администрирования отдельно от других параметров Сервера администрирования, чтобы перенести Сервер администрирования с одного устройства на другое без потери данных.

Мобильные сертификаты

Мобильный сертификат ("M") необходим для аутентификации Сервера администрирования на мобильных устройствах. Вы указываете мобильный сертификат в свойствах Сервера администрирования.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Open Single Management Platform автоматически генерирует этот сертификат за 90 дней до истечения срока действия общего сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификация), вы генерируете эти сертификаты с помощью доверенного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, в свойствах Сервера администрирования можно указать пользовательские сертификаты, выпущенные другим доверенным центром сертификации, при условии, что интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Сертификат Веб-сервера

Веб-сервер является компонентом Сервера администрирования Kaspersky Security Center и использует специальный тип сертификата. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства. Для этого Веб-сервер может использовать различные сертификаты.

Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли OSMP.

2. Общий сертификат Сервера администрирования ("C").

Сертификат Консоли OSMP

Сервер Консоли OSMP имеет собственный сертификат. Когда вы открываете сайт, браузер проверяет, является ли ваше соединение надежным. Сертификат Web Console позволяет аутентифицировать Web Console и используется для шифрования трафика между браузером и Web Console.

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Консоли OSMP не является приватным и что сертификат Консоли OSMP недействителен. Это предупреждение появляется потому, что сертификат Консоли OSMP является самоподписанным и автоматически генерируется Open Single Management Platform. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

- Замените сертификат Kaspersky Security Center Web Console на пользовательский сертификат (рекомендуемый параметр). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.

- Добавить сертификат Web Console в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Требования к пользовательским сертификатам, используемым в Open Single Management Platform

В таблице ниже представлены требования к пользовательским сертификатам, предъявляемые к различным компонентам Open Single Management Platform.

Требования для сертификатов Open Single Management Platform

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера, аутентификация клиента. Сертификат должен включать допустимое альтернативное имя субъекта (Subject Alternative Name, SAN), которое содержит адрес Сервера администрирования для обратной связи: • Для IPv4: 127.0.0.1 • Для IPv6: 0:0:0:0:0:0:0:1	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
Мобильный сертификат, Мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: true. • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (EKU) (необязательно): аутентификация Сервера.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.
Сертификат, выпущенный доверенным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: true. • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.

Тип сертификата	Требования	Комментарии
Сертификат Веб-сервера	Расширенное использование ключа (EKU): аутентификация сервера. Контейнер PKCS #12 / PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	—
Сертификат Консоли OSMP	Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Консолью OSMP.
Промежуточный сертификат для публичных служб Kaspersky EDR Expert	Контейнер PEM, содержащий полную цепочку сертификатов (или только один сертификат) и незашифрованный закрытый ключ. Промежуточный сертификат должен быть выдан инфраструктурой закрытых ключей вашей организации (PKI). Максимальный срок действия пользовательского промежуточного сертификата должен быть 399 дней или больше.	—

Перевыпуск сертификата для Консоли OSMP

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Консоли OSMP равен 397 дням. Вы можете заменить существующий сертификат, полученный от доверенного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Консоли OSMP.

> Автоматический перевыпуск сертификата для OSMP не поддерживается. Вам необходимо вручную перевыпустить сертификат.

Когда вы открываете Консоль OSMP, браузер может информировать вас о том, что подключение к Консоли OSMP не является приватным и что сертификат Консоли OSMP недействителен. Это предупреждение появляется потому, что сертификат Консоли OSMP является самоподписанным и автоматически генерируется Open Single Management Platform. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

- Укажите пользовательский сертификат при его повторном выпуске (рекомендуемый вариант). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
- Добавьте сертификат Консоли OSMP в список доверенных сертификатов браузера после перевыпуска сертификата. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Чтобы перевыпустить просроченный сертификат Консоли OSMP:

Переустановите Консоль OSMP, выполнив одно из следующих действий:

- Если вы хотите использовать тот же установочный файл Консоли OSMP, удалите Консоль OSMP и установите ту же версию Консоли OSMP.
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления.

Сертификат Консоли OSMP перевыпущен со сроком действия 397 дней.

Замена сертификата для OSMP Console

По умолчанию при установке Сервера OSMP Console (далее также OSMP Console Server) сертификат браузера для приложения выпускается автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

Чтобы назначить пользовательский сертификат OSMP Console:

1. Сохраните файл с сертификатом и файл с закрытым ключом в каталоге:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   > Поддерживаемый формат файлов: PEM.
   > Пользователь с правами root имеет право на чтение и запись в каталоге. Пользователь, от имени которого запускается сервис интерактивной веб-консоли, имеет право только на чтение.

2. Присвойте файлам следующие имена:

   - web-console.crt – файл с сертификатом;
   - web-console.key – файл с закрытым ключом без пароля.

   Пользовательский основной сертификат назначен и Web Console использует его.

Если вы захотите заменить пользовательский сертификат:

- на другой пользовательский, выполните эту же инструкцию.
- на самоподписанный, удалите один либо оба файла пользовательского сертификата.

По истечении срока действия пользовательского сертификата Web Console отображает соответствующее уведомление и продолжает использовать истекший сертификат.

Если заданный вами пользовательский основной сертификат недействителен, Web Console отображает соответствующее уведомление, выпускает самоподписанный основной и переключается на него.

Уведомление начинает отображаться за 14 дней до истечения сертификата.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в OSMP Console, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <имя_файла.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <имя_файла.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же папке, где хранится файл PFX.

3. OSMP Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки OSMP Console.

Сценарий: задание пользовательского сертификата Сервера администрирования

Вы можете назначить пользовательский сертификат Сервера администрирования, например, для лучшей интеграции с существующей инфраструктурой открытых ключей (PKI) вашей организации или для пользовательской конфигурации параметров сертификата. Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования.

> Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Предварительные требования

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен доверенным центром сертификации (CA). Также новый сертификат должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением pfx или p12. Для нового сертификата должны быть соблюдены требования, перечисленные ниже.

Тип сертификата: Общий сертификат, общий резервный сертификат ("C", "CR")

Требования:

- Минимальная длина ключа: 2048.
- Основные ограничения:
  - CA: true.
  - Ограничение длины пути: Отсутствует.

    Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
- Использование ключа:
  - Цифровая подпись.
  - Подпись сертификата.
  - Шифрование ключей.
  - Подписывание списка отзыва (CRL).
- Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера и аутентификация клиента. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера и клиента должны быть указаны в EKU.
- Сертификат должен содержать действительное альтернативное имя субъекта (SAN).
- В поле `subjectAltName` должен быть указан loopback-адрес Сервера администрирования:
  - Для IPv4: 127.0.0.1
  - Для IPv6: 0:0:0:0:0:0:0:1

Сертификаты, выпущенные доверенным центром сертификации (англ. certificate authority, CA), не имеют разрешения на подписывание сертификатов. Чтобы использовать такие сертификаты, убедитесь, что на точках распространения или шлюзах соединения в вашей сети установлен Агент администрирования версии 13 или выше. В противном случае вы не сможете использовать сертификаты без разрешения на подпись.

Этапы

Указание сертификата Сервера администрирования состоит из следующих этапов:

1. **Замена сертификата Сервера администрирования**

   Используйте для этой цели утилиту командной строки klsetsrvcert.

2. **Указание нового сертификата и восстановление связи Агентов администрирования с Сервером администрирования**

   При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы указать новый сертификат и восстановить соединение, используйте командную строку утилиты klmover.

Результаты

После завершения сценария сертификат Сервера администрирования будет заменен, Агент администрирования на управляемых устройствах аутентифицирует сервер с использованием нового сертификата.

Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

Чтобы заменить сертификат Сервера администрирования,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke ksc --action klsetsrvcert \
  --param ksc_server_certificate="<путь к новому сертификату>" \
  --param ksc_server_cert_pass="<пароль>"
```

где:

- `<путь к новому сертификату>` – путь к контейнеру с сертификатом и закрытому ключу в формате PKCS#12 (файл с расширением .p12 или .pfx).
- `<пароль>` – пароль, который используется для защиты контейнера PKCS # 12. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.

  Если пароль содержит двойные кавычки, используйте обратную косую черту (`\"`).

По умолчанию параметры проверки сертификата не указаны, используется пользовательский сертификат без разрешения на подпись. Вы можете заменить общий сертификат для порта 13000.

Вам не нужно загружать утилиту klsetsrvcert. Он включен в кластер Kubernetes и недоступен для прямого запуска. Утилиту klsetsrvcert можно запустить только с помощью KDT с устройства администратора.

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

После замены сертификата Сервера администрирования с помощью утилиты командной строки klsetsrvcert вам необходимо установить SSL-соединение между Агентами администрирования и Сервером администрирования, так как соединение разорвано.

Чтобы указать новый сертификат Сервера администрирования и восстановить соединение:

В командной строке выполните следующую команду:

```
klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>]
```

Эта утилита автоматически копируется в папку установки Агента администрирования при установке Агента администрирования на клиентское устройство.

Описание параметров утилиты klmover представлено в таблице ниже.

Значения параметров утилиты klmover

Параметр	Значение
`-address < адрес Сервера >`	Адрес Сервера администрирования для подключения. В качестве адреса можно указать IP-адрес или DNS-имя.
`-pn < номер порта >`	Номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования. По умолчанию установлен порт 14000.
`-ps < номер SSL-порта >`	Номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию установлен порт 13000. Для корневого Сервера администрирования используется порт 13000, и изменить его нельзя.
`-nossl`	Использовать незашифрованное подключение к Серверу администрирования. Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.
`-cert < путь к файлу сертификата >`	Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

Иерархия Серверов администрирования

Некоторые компании-клиенты, например MSP-клиенты, могут использовать несколько Серверов администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования на разных уровнях иерархии. Корневой Сервер администрирования может действовать только как главный Сервер.

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики, задачи, роли пользователей и инсталляционные пакеты, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты и выборки событий на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.
- Главный Сервер администрирования может использоваться в качестве источника обновлений для подчиненного Сервера администрирования.

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux. Корневой Сервер администрирования может действовать только как главный Сервер.

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

Чтобы добавить Сервер администрирования, доступный для подключения через Консоль OSMP, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. Перейдите в свойства будущего главного Сервера администрирования:
   a. В главном меню выберите любой раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.
   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.
3. В открывшемся окне свойств перейдите на вкладку **Серверы администрирования**.
4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.

5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. Заполните следующие поля:

   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

   - **Адрес подчиненного Сервера администрирования (необязательно)**

     Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

     Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   - **SSL-порт Сервера администрирования**

     Укажите номер SSL-порта главного Сервера администрирования. По умолчанию установлен порт 13000.

     Для корневого Сервера администрирования используется порт 13000, и изменить его нельзя.

   - **API-порт Сервера администрирования**

     Номер порта, который Web Console будет использовать для приема подключений от подчиненного Сервера администрирования по OpenAPI. По умолчанию установлен порт 13299.

     При построении иерархии Web Console подключается к будущему подчиненному Серверу, запрашивает учетные данные, получает открытый сертификат и выполняет первоначальную настройку.

     После построения иерархии Сервера администрирования порт 13299 больше не будет использоваться. Серверы администрирования будут взаимодействовать через порт 13000.

   - **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

     Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

     Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

7. Укажите сертификат будущего подчиненного Сервера.

   Работа мастера завершена.

8. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

   Файл сертификата находится на будущем главном Сервере администрирования, /var/opt/kaspersky/klnagent_srv/1093/cert/.

9. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

   a. Нажмите на имя Сервера администрирования.

   b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на вкладке **Общие**.

   c. Выберите параметр **Этот Сервер администрирования является подчиненным в иерархии**.

   > Корневой Сервер администрирования может действовать только как главный Сервер.

   d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

   e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

   f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   g. Если подключение к будущему главному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

   h. Нажмите на кнопку **Сохранить**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Просмотр списка подчиненных Серверов администрирования

Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:

1. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**).

2. В верхней части страницы нажмите на кнопку **Показать иерархию**.

   В открывшейся панели навигации отобразится список подчиненных (в том числе виртуальных) Серверов администрирования. Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

> Вы не сможете перейти к виртуальным Серверам администрирования, если вы открыли панель навигации из разделов **IP-диапазоны** и **Удаленные объекты**.
> Также отображаются группы администрирования. Группы доступны для управления, если вы открыли панель навигации из следующих разделов: **Активы (Устройства)**, **Политики**, **Задачи** и **Точки распространения**. Иначе группы отображаются серым цветом.

Если вы подключены к главному Серверу администрирования в OSMP Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку OSMP Console, добавив подчиненный Сервер в список доверенных Серверов администрирования** После этого вы сможете подключиться к виртуальному Серверу администрирования в OSMP Console.

  1. На устройстве, где установлено приложение OSMP Console, запустите установочный файл OSMP Console, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте OSMP Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в OSMP Console.

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования;
- включение и выключение виртуальных Серверов администрирования;
- назначение администратора виртуального Сервера администрирования;
- смена Сервера администрирования для клиентских устройств;
- удаление виртуальных Серверов администрирования.

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
   Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:
   - **Имя виртуального Сервера администрирования**.
   - **Адрес подключения Сервера администрирования**.
     Вы можете указать имя или IP-адрес Сервера администрирования.
6. Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать новую учетную запись.

   При необходимости вы можете создать учетную запись, которая будет выполнять роль администратора виртуального Сервера администрирования с помощью утилиты kladduser. Для этого используйте следующую команду:

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   Где virtual_server_name – имя виртуального Сервера администрирования.
7. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Если вы подключены к главному Серверу администрирования в OSMP Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку OSMP Console, добавив подчиненный Сервер в список доверенных Серверов администрирования** После этого вы сможете подключиться к виртуальному Серверу администрирования в OSMP Console.

  1. На устройстве, где установлено приложение OSMP Console, запустите установочный файл OSMP Console, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. Выберите параметр **Обновить**.

3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте OSMP Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в OSMP Console.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

Чтобы включить или выключить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.

3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.

4. В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

   Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в OSMP Console, администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. OSMP Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан.
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции** → **Права пользователей**.

Настройка прав доступа вручную

Чтобы назначить администратора виртуального Сервера администрирования:

1. Переключитесь на нужный виртуальный Сервер администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   > Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.

2. Перейдите в свойства Сервера администрирования, нажав на его имя в главном меню.

   Или в панели наведите курсор мыши на название нужного виртуального Сервера администрирования и нажмите на значок параметров (⚙).

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.

4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **OK**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - право **Чтение** в функциональной области **Общие функции** → **Базовая функциональность**.
   - право **Чтение** в функциональной области **Общие функции** → **Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

Чтобы назначить администратора нескольким виртуальным Серверам администрирования:

1. В главном окне приложения нажмите на имя главного Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Права доступа** и нажмите **Назначить**.

   В открывшемся окне **Добавить пользователей или группы** установите флажок рядом с пользователем, которого вы хотите назначить администратором.

3. Вы можете перейти на вкладку **Группы**, чтобы выбрать группы пользователей.

4. Нажмите на кнопку **Далее**.

5. Выберите серверы, для которых вы хотите назначить администратора, и нажмите **Далее**.

6. Выберите роли администратора, которые вы хотите назначить пользователю, если это необходимо.

   Если вы хотите установить пользовательские роли для текущего Сервера администрирования, перейдите в свойства нужного Сервера администрирования, нажмите **Назначить роли** и выберите пользовательские роли.

7. Нажмите на кнопку **Готово**, чтобы сохранить изменения.

Администратор с выбранными ролями теперь назначен нескольким виртуальным Серверам администрирования.

Чтобы отозвать права доступа администратора:

1. Переключитесь на нужный Сервер администрирования.

2. В главном окне приложения нажмите на имя Сервера администрирования.

3. На открывшейся странице перейдите на вкладку **Права доступа**.

4. Установите флажок рядом с пользователем, у которого вы хотите отозвать права доступа.

5. Нажмите **Отозвать** и подтвердите действие.

   Права доступа выбранного пользователя отозваны.

Настройка прав доступа с помощью назначения пользовательских ролей

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:

1. На главном Сервере администрирования создайте пользовательскую роль и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.

2. Переключитесь на нужный виртуальный Сервер администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   > Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.

3. Назначьте новую роль или несколько ролей учетной записи администратора.

   Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области, вы можете настроить доступ к определенным объектам на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи *Смена Сервера администрирования*. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования.

> Вы не можете использовать задачу *Смена Сервера администрирования* для клиентских устройств, подключенных к Серверу администрирования через шлюзы соединения. Для таких устройств необходимо перенастроить Агент администрирования или переустановить Агент администрирования, указав шлюз соединения.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Open Single Management Platform**.

   b. В поле **Тип задачи** выберите **Смена Сервера администрирования**.

   c. В поле **Название задачи** укажите название создаваемой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

   d. Выберите устройства, которым будет назначена задача:

   Назначить задачу группе администрирования

   Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

   Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

   Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   Задать адреса устройств вручную или импортировать из списка

   Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

   Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   Назначить задачу выборке устройств

   Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

   Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. На шаге мастера **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

5. На этом шаге мастера подтвердите свое согласие с условиями смены Сервера администрирования для клиентских устройств.

6. На этом шаге мастера выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами:

   Смена главного Сервера администрирования

   Чтобы переместить клиентские устройства на другой главный Сервер администрирования, укажите следующие параметры подключения к Серверу администрирования:

   1. В поле **Адрес Сервера администрирования** укажите адрес нового главного Сервера администрирования.

   2. В поле **Номер порта** укажите номер порта для подключения к Серверу администрирования.

      По умолчанию установлен порт 14000.

   3. В поле **SSL-порт** укажите номер SSL-порта главного Сервера администрирования.

      По умолчанию установлен порт 13000.

   4. При необходимости включите параметр **Использовать прокси-сервер**.

      Если этот параметр выключен, для подключения устройства к Серверу администрирования используется прямое соединение.

      Если этот параметр включен, укажите параметры прокси-сервера:

      - **Адрес прокси-сервера**

      - **Порт прокси-сервера**

      Если ваш прокси-сервер требует аутентификации, в полях **Имя пользователя** и **Пароль** укажите учетные данные учетной записи, под которой устанавливается соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

   5. При необходимости загрузите новый сертификат Сервера администрирования.

   Смена виртуального Сервера на этом главном Сервере

   Выберите этот параметр, чтобы переместить на виртуальный Сервер администрирования клиентские устройства на текущем главном Сервере администрирования. Для этого в раскрывающемся списке **Имя виртуального Сервера администрирования** выберите нужный виртуальный Сервер администрирования.

7. На шаге мастера **Выбор учетной записи для запуска задачи** укажите параметры учетной записи:

   Учетная запись по умолчанию

   Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

   По умолчанию выбран этот вариант.

   Задать учетную запись

   В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

Учетная запись

Учетная запись, от имени которой будет запускаться задача.

Пароль

Пароль учетной записи, от имени которой будет запускаться задача.

8. Если требуется изменить параметры задачи по умолчанию, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**.

   Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. Если вы хотите изменить параметры задачи по умолчанию, в окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky EDR Expert, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. Переключитесь на главный физический Сервер администрирования, которому принадлежит виртуальный Сервер администрирования:

   a. В главном меню выберите любой раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели нажмите на имя нужного главного физического Сервера администрирования.

      В главном меню Сервер администрирования изменится на тот, который вы выбрали.

2. Перейдите к свойствам главного физического Сервера администрирования одним из следующих способов:

   - В панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

   - В главном окне приложения нажмите на имя Сервера администрирования.

3. В открывшемся окне свойств страницы выберите вкладку **Серверы администрирования**.

4. Выберите виртуальный Сервер администрирования, который вы хотите удалить.

5. В строке меню нажмите на кнопку **Удалить**.

   Виртуальный Сервер администрирования удален.

Настройка журнала событий подключения к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

Чтобы настроить регистрацию событий подключения к Серверу администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

   Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **Сохранить**.

Также вы можете выполнить следующее:

- Изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи.

- Уменьшить или выключить период хранения для событий Сервера администрирования, Агента администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Изменение учетных данных СУБД

Иногда может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

Изменение учетных данных базы данных Сервера администрирования

Чтобы изменить учетные данные базы данных Сервера администрирования и базы данных IAM в среде Linux:

1. Остановите Сервер администрирования. В зависимости от типа развертывания Kaspersky Security Center Linux под учетной записью root выполните одну из следующих команд:

   - Для отказоустойчивого кластера Kaspersky Security Center Linux:

     На активном узле выполните следующую команду:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

- Для георасределенного отказоустойчивого кластера Kaspersky Security Center Linux:

  На обоих узлах выполните следующую команду:

  ```
  crm node standby
  ```

- Для развертывания Сервера администрирования не кластерной конфигурации:

  Выполните следующие команды:

  ```
  systemctl stop kladminserver_srv.service
  systemctl stop kliam_srv.service
  ```

2. Подключитесь к базе данных Сервера администрирования с правами суперпользователя СУБД и выполните следующую команду:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   где `<old_kscdbadmin>` – предыдущая учетная запись СУБД, которую Сервер администрирования использовал для подключения к своей базе данных, а `<new_kscdbadmin>` – новая учетная запись СУБД.

3. Подключитесь к базе данных IAM с правами суперпользователя СУБД и выполните следующую команду:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   где `<old_iamdbadmin>` – предыдущая учетная запись СУБД, которую Сервер администрирования использовал для подключения к своей базе данных, и `<new_iamdbadmin>` – это новые учетные записи СУБД.

4. Откройте конфигурационный файл IAM /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml.

5. В секции `dbms_iam` укажите новые учетные данные в полях user и password. Убедитесь, что учетная запись существует в СУБД и указана как владелец базы данных IAM.

6. Запустите Сервер администрирования. В зависимости от типа развертывания Kaspersky Security Center Linux под учетной записью root выполните одну из следующих команд:

   - Для отказоустойчивого кластера Kaspersky Security Center Linux:

     На активном узле выполните следующую команду:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - Для георасределенного отказоустойчивого кластера Kaspersky Security Center Linux:

     На обоих узлах выполните следующую команду:

     ```
     crm node online
     ```

- Для развертывания Сервера администрирования не кластерной конфигурации:

  Выполните следующие команды:

  ```
  systemctl start kladminserver_srv.service
  systemctl start kliam_srv.service
  ```

7. Запустите утилиту klsrvconfig:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. Укажите новое имя учетной записи. Вам нужно указать учетные данные учетной записи, которая существует в СУБД.

9. Введите новый пароль.

10. Укажите этот новый пароль для подтверждения.

11. Дождитесь возобновления работы Сервера администрирования и появления записи в syslog о том, что Сервер администрирования готов к работе с графическим интерфейсом пользователя.

Учетные данные базы данных Сервера администрирования изменены.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.

3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.

4. В меню выберите пункт **Удалить**.

5. В открывшемся окне нажмите на кнопку **OK** для подтверждения удаления подчиненного Сервера администрирования.

Бывший главный и бывшие подчиненные Серверы администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Open Single Management Platform может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8).
2. Cloudflare DNS (1.1.1.1).
3. Alibaba Cloud DNS (223.6.6.6).
4. Quad9 DNS (9.9.9.9).
5. CleanBrowsing (185.228.168.168).

Запросы к DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Open Single Management Platform использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

Чтобы настроить использование публичного DNS с помощью утилиты klscflag:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду, чтобы выключить использование публичного DNS:

   ```
   ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
   ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1'
   ```

2. Чтобы включить использование публичного DNS, выполните команду:

   ```
   ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
   ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0'
   ```

Настройка интерфейса

Вы можете настроить интерфейс Консоли OSMP на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

Чтобы настроить интерфейс Консоли OSMP в соответствии в соответствии с используемым в настоящее время набором функций:

1. В главном окне приложения перейдите в раздел **Параметры** → **Параметры интерфейса**.
2. Включите или выключите параметр **Показать раздел "Шифрование и защита данных"**.
3. Нажмите на кнопку **Сохранить**.

   После включения требуемых параметров Консоль отображает соответствующие разделы в главном меню.

Шифрование подключения TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием TLS-протокола. Вы можете включить протоколы шифрования TLS и поддерживаемые наборы шифрования на Сервере администрирования. Open Single Management Platform поддерживает TLS-протокол версий 1.0, 1.1, 1.2 и 1.3. Вы можете выбрать требуемый протокол шифрования и наборы шифрования.

Open Single Management Platform использует самоподписанные сертификаты. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные доверенным центром сертификации.

Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования:

1. На устройстве администратора, на котором расположена утилита KDT, выполните команду:

   ```
   ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
   ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <значение> -t d'
   ```

   Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования.

   Укажите параметр <value> флага SrvUseStrictSslSettings:

   - 4 – включены только TLS-протоколы версий 1.2 и 1.3. Также включены наборы шифрования с TLS_RSA_WITH_AES_256_GCM_SHA384 (эти наборы шифрования необходимы для обратной совместимости с Kaspersky Security Center 11). Это значение по умолчанию.

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (с набором шифрования TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Наборы шифрования поддерживаемые TLS-протоколом 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5 – включены только TLS-протоколы версий 1.2 и 1.3. Для TLS-протоколов версий 1.2 и 1.3 поддерживаются определенные наборы шифрования, перечисленные ниже.

Наборы шифрования поддерживаемые TLS-протоколом 1.2:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Не рекомендуется использовать значения 0, 1, 2 или 3 для значений параметра флага SrvUseStrictSslSettings. Эти значения параметров соответствуют небезопасным версиям TLS-протокола (протоколы TLS 1.0 и TLS 1.1) и небезопасным наборам шифрования и используются только для обратной совместимости с более ранними версиями Kaspersky Security Center.

2. Перезапустите следующие службы Open Single Management Platform:

- службу Сервера администрирования;
- службу Веб-сервера;
- службу активации прокси-сервера.

Шифрование трафика с помощью TLS-протокола включено.

Вы можете использовать флаги KLTR_TLS12_ENABLED и KLTR_TLS13_ENABLED, чтобы включить поддержку TLS-протоколов 1.2 и 1.3 соответственно. Эти флаги включены по умолчанию.

Чтобы включить или выключить поддержку TLS-протоколов 1.2 и 1.3,

На устройстве администратора, на котором расположена утилита KDT, выполните одну из следующих команд:

- Чтобы включить или выключить поддержку TLS-протокола 1.2:

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <значение> -t d'
```

- Чтобы включить или выключить поддержку TLS-протокола 1.3:

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <значение> -t d'
```

Укажите параметр < значение > флага:

- 1 – чтобы включить поддержку TLS-протокола.
- 0 – чтобы выключить поддержку TLS-протокола.

Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Open Single Management Platform позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования и его подчиненных Серверов администрирования;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов администрирования.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

Обнаружение сетевых устройств состоит из следующих этапов:

1. **Первоначальное обнаружение устройств**

   Выполните обнаружение устройств вручную.

2. **Настройка будущих опросов**

   Убедитесь, что опрос IP-диапазонов включен и что расписание опроса соответствует требованиям вашей организации. При настройке расписания опроса опирайтесь на рекомендации для периодичности опросов сети.

   Также можно включить опрос Zeroconf, если в вашей сети есть IPv6-устройства.

   Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена.

   Используйте точки распространения с операционной системой Windows для опроса сетей Windows.

   > Вы можете выполнять опрос IP-диапазонов и опрос Zeroconf только с помощью точки распространения.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. При необходимости можно настроить правила автоматического перемещения этих устройств в группу **Управляемые устройства**. Можно также настроить правила хранения.

   Если вы пропустили этап, на котором задаются правила, все новые обнаруженные устройства будут помещены в группу **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.

Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Опрос сети Windows

Об опросе сети Windows

Сервер администрирования Kaspersky EDR Expert не поддерживает опрос сети Windows. Используйте точки распространения с операционной системой Windows для опроса сетей Windows.

При быстром опросе точки распространения получают только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- имя операционной системы;
- IP-адрес;
- DNS-имя;
- NetBIOS-имя.

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен;

- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Опрос IP-диапазонов

Kaspersky EDR Expert позволяет опрашивать IP-диапазоны только с помощью точки распространения. Точка распространения пытается выполнить обратное преобразование имен: для каждого IPv4-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, точка распространения отправляет запрос `ICMP ECHO REQUEST` (аналог команды `ping`) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Kaspersky EDR Expert. Обратное преобразование имен необходимо для исключения сетевых устройств, которые могут иметь IP-адреса, но не являются компьютерами, таких как сетевые принтеры или роутеры.

Этот способ опроса основывается на правильно настроенной локальной службе DNS. Для его использования должна быть настроена зона обратного просмотра DNS. Если эта зона не настроена, опрос IP-подсети не даст результатов.

Первоначально точка распространения получает IP-диапазоны для опроса из сетевых параметров устройства, которое выполняет роль точки распространения. Если адрес устройства 192.168.0.1 и маска подсети – 255.255.255.0, сеть 192.168.0.0/24 включена в список адресов для автоматического опроса. Точка распространения выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Если включен только опрос IP-диапазонов, точка распространения обнаруживает устройства только с IPv4-адресами. Если в вашей сети есть IPv6-устройства, включите опрос Zeroconf устройств.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory или Samba укажите `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Опрос IP-диапазонов с помощью точки распространения

Чтобы настроить опрос IP-диапазонов с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Перейдите в раздел **Опрос IP-диапазонов** и выберите параметр **Разрешить опрос диапазона**.

   Откроется окно **IP-диапазон**
3. Укажите имя нового IP-диапазона.

4. Нажмите на кнопку **Добавить** и укажите IP-диапазон с помощью адреса и маски подсети или с помощью начального и конечного IP-адреса. Также можно добавить существующую подсеть, нажав на кнопку **Обзор**.

5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

   Варианты расписания опроса:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

   - **Ежемесячно в выбранный день**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

     По умолчанию параметр выключен.

6. Включите параметр **Использовать Zeroconf для опроса IPv6-сетей**, чтобы точка распространения выполняла опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*).

   В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

После завершения опроса вновь обнаруженные устройства автоматически включаются в группу **Управляемые устройства**, если вы настроили и включили правила перемещения устройств. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Опрос контроллеров домена

Open Single Management Platform поддерживает опрос следующих типов контроллеров домена:

- Microsoft Active Directory.
- Samba.
- FreeIPA.
- ALD Pro.

Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4.

При опросе контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

Предварительные требования

Перед опросом контроллеров домена убедитесь, что включены следующие протоколы:

- Simple Authentication and Security Layer (SASL).
- Lightweight Directory Access Protocol (LDAP).

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для SASL.
- 636 для TLS.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory, Samba, FreeIPA или ALD Pro вам нужно указать `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

> Если домен Microsoft Active Directory содержит несколько контроллеров домена, выбор конкретного контроллера во время опроса домена не поддерживается. Соединение устанавливается с первым обнаруженным контроллером домена. Для обеспечения корректной аутентификации в домене Microsoft Active Directory поле альтернативного имени субъекта (SAN) сертификата должно включать все адреса контроллеров домена, входящих в этот домен, а также NetBIOS-имя домена Microsoft Active Directory.

Опрос контроллеров домена с помощью Сервера администрирования

Чтобы опросить контроллеры домена с помощью Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.

2. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно **Параметры опроса контроллеров домена**.

3. В поле **Опрос** установите переключатель в положение **Включено**.

4. В разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, укажите адрес и учетные данные пользователя контроллеров домена, а затем нажмите **OK**.

5. В окне **Параметры опроса контроллеров домена** выполните следующие действия:

   - Выберите тип опроса контроллера домена: **Active Directory или Samba 4**, **FreeIPA**, **ALD Pro**.

   - При необходимости настройте расписание опроса. По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждые N дней**

       Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

       По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

     - **Каждые N минут**

       Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

     - **По дням недели**

       Опрос выполняется регулярно, в указанные дни недели, в указанное время.

     - **Ежемесячно в выбранный день**

       Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

     - **Запускать пропущенные задачи**

       Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

       Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

       Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

       По умолчанию параметр выключен.

Если вы измените учетные записи пользователей в группе безопасности домена, эти изменения отобразятся в Open Single Management Platform через час после опроса контроллеров домена.

6. При необходимости измените тенанта, который будет назначен обнаруженным учетным записям. Для этого выберите нужный тенант из раскрывающегося списка **Тенант**.

   По умолчанию указан тенант Сервера администрирования. Вы можете выбрать несколько тенантов.

7. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

8. Если требуется запустить опрос сети немедленно, нажмите на кнопку **Начать опрос**.

Опрос контроллеров домена с помощью точки распространения

Также можно опрашивать контроллеры домена с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос для всех типов контроллеров домена.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения.

2. Выберите раздел **Опрос контроллеров домена**.

3. В поле **Опрос** установите переключатель в положение **Включено**.

4. Если вы используете точку распространения с операционной системой Linux, выберите тип опроса контроллера домена: **Active Directory или Samba 4**, **FreeIPA**, **ALD Pro**.

   Необязательно указывать один и тот же тип контроллера домена при настройке опроса с помощью точки распространения и с помощью Сервера администрирования.

5. Выберите контроллеры домена, которые вы хотите опросить.

   Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллеров домена.

   Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

   - **Опросить текущий домен**
   - **Опросить весь лес доменов**
   - **Опросить указанные домены**

6. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Консоли OSMP по протоколу Kerberos.

Аутентификация и подключение к контроллеру домена

При первоначальном подключении к контроллеру домена Сервер администрирования идентифицирует протокол подключения. Этот протокол используется для всех будущих подключений к контроллеру домена.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Сервер администрирования пытается подключиться к контроллеру домена по TLS.

   По умолчанию проверка сертификата не требуется. Для флага KLNAG_LDAP_TLS_REQCERT установите значение 1, чтобы принудительно выполнить проверку сертификата.

   По умолчанию для доступа к цепочке сертификатов используется зависящий от операционной системы путь к центру сертификации (CA). Используйте флаг KLNAG_LDAP_SSL_CACERT, чтобы указать другой путь.

2. В случае сбоя TLS-соединения Сервер администрирования пытается подключиться к контроллеру домена по SASL (DIGEST-MD5).

3. В случае сбоя подключения по SASL (DIGEST-MD5) Сервер администрирования использует простую проверку подлинности (Simple Authentication) по незашифрованному TCP-соединению для подключения к контроллеру домена.

Вы можете использовать команды KDT для настройки флагов. Например, вы можете принудительно проверить сертификат. Для этого на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
KLNAG_LDAP_TLS_REQCERT -t d -v 1'
```

Настройка контроллеров домена Samba

Open Single Management Platform поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

> Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Open Single Management Platform и контроллером домена Samba.

Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:

1. Выполните следующую команду, чтобы использовать расширение схемы RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   > Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

Для всех устройств с операционной системой Linux в контроллере домена Samba в файле `/etc/samba/smb.conf` нужно указать `netbios name` и параметры `workgroup`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky EDR Expert обнаруживает временные виртуальные машины и добавляет информацию о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Также несуществующие виртуальные машины могут отображаться в OSMP Console.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky EDR Expert реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

Чтобы включить динамический режим VDI:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства**.
3. В окне **Свойства** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** выберите параметр **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

Перемещение в группу администрирования устройств, являющихся частью VDI

Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования:

1. Перейдите в раздел **Управление активами** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. На вкладке **Условия правила** выберите вкладку **Виртуальные машины**.
4. Установите для правила **Является виртуальной машиной** значение **Да** и для **Часть Virtual Desktop Infrastructure** значение **Да.**
5. Нажмите на кнопку **Сохранить**.

Управление клиентскими устройствами

Kaspersky EDR Expert позволяет управлять клиентскими устройствами:

- Просматривать параметры и статусы управляемых устройств, в том числе кластеров и массивов серверов.
- Настраивать точки распространения.
- Управлять задачами.

Группы администрирования можно использовать для объединения клиентских устройств в набор, которым можно управлять как единым целым. Клиентское устройство может быть включено только в одну группу администрирования. Устройства могут быть автоматически отнесены к группе на основе **Условия правила**:

- Создание правил перемещения устройств.
- Копирование правил перемещения устройств.
- Условия для правила перемещения устройств.

Вы можете использовать выборки устройств, чтобы для фильтровать устройства по условию. Вы также можете назначать теги устройствам для создания выборок устройств, поиска устройств и распределения устройств между группами администрирования.

Параметры управляемого устройства

Чтобы просмотреть параметры управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

Общие

Эта вкладка содержит следующие разделы:

- Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:
  - **Имя**

    В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.
  - **Описание**

    В поле можно ввести дополнительное описание клиентского устройства.
  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.
  - **Полное название группы**

    Группа администрирования, в состав которой входит клиентское устройство.
  - **Последнее обновление антивирусных баз**

Дата последнего обновления антивирусных баз или приложений на устройстве.

- **Соединение с Сервером администрирования**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Последнее появление в сети**

  Дата и время, когда устройство последний раз было видимо в сети.

- **Версия Агента администрирования**

  Версия установленного Агента администрирования.

- **Создано**

  Дата создания устройства в Open Single Management Platform.

- **Владелец устройства**

  Имя владельца устройства. Вы можете назначить или удалить пользователя в качестве владельца устройства, нажав на ссылку **Сменить владельца устройства**.

- **Не разрывать соединение с Сервером администрирования**

  Если этот параметр включен, сохраняется постоянное соединение между управляемым устройством и Сервером администрирования. Вы можете использовать этот параметр, если не используете push-серверы, которые обеспечивают такое соединение.

  Если параметр выключен и push-серверы не используются, управляемое устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

  Этот параметр по умолчанию выключен на управляемых устройствах. Этот параметр включен по умолчанию на устройстве, на котором установлен Сервер администрирования, и остается включенным, даже если вы попытаетесь его выключить.

- В разделе **Сеть** отображается следующая информация о сетевых свойствах клиентского устройства:

  - **IP-адрес**

    IP-адрес устройства

  - **Windows-домен**

    Рабочая группа, содержащая устройство.

  - **DNS-имя**

    Имя DNS-домена клиентского устройства.

  - **NetBIOS-имя**

    NetBIOS-имя клиентского устройства.

  - **IPv6-адрес**

- В разделе **Система** представлена информация об операционной системе, установленной на клиентском устройстве:
  - **ОС**
  - **Архитектура процессора**
  - **Имя устройства**
  - **Тип виртуальной машины**

    Производитель виртуальной машины
  - **Динамическая виртуальная машина как часть VDI**

    В этой строке показано, является ли клиентское устройство динамической виртуальной машиной как часть VDI.
- В разделе **Защита** представлена следующая информация о состоянии антивирусной защиты на клиентском устройстве:
  - **Видимо в сети**

    Статус видимости клиентского устройства.
  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.
  - **Описание статуса**

    Статус защиты клиентского устройства и подключения к Серверу администрирования.
  - **Состояние защиты**

    Статус текущего состояния постоянной защиты клиентского устройства.

    После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.
  - **Последняя полная проверка**

    Дата и время последнего поиска вредоносного ПО на клиентском устройстве.
  - **Обнаружен вирус**

    Общее количество обнаруженных на клиентском устройстве угроз с момента установки приложения безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.
  - **Объекты, которые не удалось вылечить**

    Количество необработанных файлов на клиентском устройстве.

    В поле не учитывается количество необработанных файлов для мобильных устройств.
  - **Статус шифрования дисков**

Текущее состояние шифрования файлов на локальных дисках устройства. Описание статусов см. в онлайн-справке Kaspersky Endpoint Security for Windows.

Файлы могут быть зашифрованы только на управляемых устройствах, на которых установлен Kaspersky Endpoint Security for Windows.

- В разделе **Статус устройства определен приложением** отображается информация о статусе устройства, который определен управляемым приложением, установленным на клиентском устройстве. Это состояние устройства может отличаться от того, которое определено Kaspersky EDR Expert.

Приложения

На этой вкладке отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. На этой вкладке находятся кнопки **Запустить** и **Остановить**, которые позволяют запускать и останавливать выбранное приложение "Лаборатории Касперского" (кроме Агента администрирования). Вы можете использовать эти кнопки, если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования. Если управляемое устройство недоступно для push-уведомлений, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** в разделе **Общие** включен), кнопки **Запустить** и **Остановить** активны. Иначе при попытке запустить или остановить приложение появится сообщение об ошибке. Также вы можете нажать на имя приложения, чтобы просмотреть общую информацию о приложении, список событий, произошедших на устройстве, и параметры приложения.

Действующие политики и профили политик

На этой вкладке отображаются списки политик и профилей политик, которые назначены управляемому устройству.

Задачи

На вкладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. Если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования, отображается статус задачи и кнопки управления задачей активны. Если push-сервер не может получить доступ к управляемому устройству, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** с Сервером администрирования в разделе **Общие** включен), действия с задачами доступны.

В случае отсутствия связи статус не отображается и кнопки неактивны.

События

На вкладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Вы можете экспортировать, копировать и удалять события устройства.

Проблемы безопасности

На вкладке **Проблемы безопасности** можно просматривать, изменять и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется приложением "Лаборатории Касперского", которое создает проблему безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

Теги

На вкладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

Дополнительно

Эта вкладка содержит следующие разделы:

- **Реестр приложений**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

  Информация об установленных приложениях предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

  При нажатии на имя приложения открывается окно, содержащее сведения о приложении и список пакетов обновлений, установленных для этого приложения.

- **Исполняемые файлы**. В этом разделе отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

- **Точки распространения**. В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

  - **Экспортировать в файл**

    По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию приложение экспортирует список устройств в файл формата CSV.

  - **Свойства**

    По кнопке **Свойства** вы можете посмотреть и настроить параметры точки распространения, с которым взаимодействует устройство.

- **Реестр оборудования**. В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

- оперативная память;
- запоминающие устройства;
- материнская плата;
- процессор;
- сетевой адаптер;
- мониторы;
- видеоадаптер;
- звуковая плата.

Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

- общий объем оперативной памяти;
- общий объем запоминающих устройств;
- материнская плата;
- процессор;
- сетевой адаптер.

- **Применимые обновления**. В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Уязвимости в приложениях**. В этом разделе можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах.

  Чтобы сохранить уязвимости в файл, установите флажки рядом с уязвимостями, которые вы хотите сохранить, и нажмите на кнопку **Экспортировать в CSV** или на кнопку **Экспортировать в TXT**.

  Раздел содержит следующие параметры:

  - **Показывать только те уязвимости, которые можно закрыть**

    Если параметр включен, в разделе отображаются уязвимости, которые можно закрыть патчем.

    Если параметр выключен, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

    По умолчанию параметр включен.

  - **Свойства уязвимости**

Нажмите на имя уязвимости в приложениях в списке, чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

- Пропустить уязвимость в приложениях на этом управляемом устройстве (в OSMP Console).
- Просмотреть список рекомендуемых исправлений для уязвимости.
- Вручную указать обновления программного обеспечения для закрытия уязвимости (в OSMP Console).
- Просмотреть экземпляр уязвимости.
- Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

- **Удаленная диагностика**. В этом разделе можно выполнять удаленную диагностику клиентских устройств.

Если вы используете СУБД PostgreSQL, MariaDB или MySQL, на вкладке **События** может отображаться неполный список событий для выбранного клиентского устройства. Это происходит, когда СУБД хранит очень большое количество событий. Вы можете увеличить количество отображаемых событий, выполнив одно из следующих действий:

- Удалить ненужные события.
- Сократить срок хранения ненужных событий.

Чтобы увидеть полный список событий, зарегистрированных на Сервере администрирования для устройства, используйте Отчеты.

Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk. Утилита klnagchk находится в папке установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты либо выводит информацию на экран.
- Пытается установить соединение Агента администрирования с Сервером администрирования.

  Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,

на устройстве с установленным Агентом администрирования запустите утилиту klnagchk из командной строки под учетной записью локального администратора.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart][-sendhb]
```

Описания ключей:

- `-logfile <имя файла>` – записывает значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.

- `-sp` – выводит пароль для аутентификации пользователя на прокси-сервере.

  Ключ используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохраняет сертификат для аутентификации доступа к Серверу администрирования в указанном файле.

- `-restart` – запускает Агент администрирования после завершения работы утилиты.

- `-sendhb` – запускает синхронизацию Агента администрирования с Сервером администрирования.

После запуска утилита klnagchk обращается к конфигурационным файлам Агента администрирования и отображает параметры подключения. Эти параметры задаются при установке Агента администрирования и в параметрах политики Агента администрирования:

- `Current device` – имя клиентского устройства в сети Windows.

- `Network Agent version` – номер версии Агента администрирования (с патчами), установленного на устройстве.

- `Server address` – адрес Сервера администрирования.

- `Use SSL` – параметр, указывающий, используется ли защищенное соединение при подключении к Серверу администрирования.

  Возможные значения:

  - 0 – защищенный канал не используется.

  - 1 – используется защищенный канал.

- `Compress traffic` – параметр, указывающий, сжимается ли трафик между клиентским устройством и Сервером администрирования.

- `Server SSL ports` – номера допустимых портов для подключения к Серверу администрирования при использовании защищенного канала.

- `Server ports` – номера портов, допустимых для подключения к Серверу администрирования при использовании обычного соединения.
- `Use proxy server` – параметр, указывающий, используется ли прокси-сервер.

  Возможные значения:

  - 0 – прокси-сервер не используется.
  - 1 – прокси-сервер используется.
- `Address` – адрес и порт прокси-сервера, разделенные двоеточием. Этот параметр отображается, только если используется прокси-сервер.
- `User name` – имя пользователя для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер.
- `Password` – пароль для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер. Чтобы показать пароль прокси-сервера, вам нужно использовать в команде ключ `sp`.
- `Certificate` – параметр, указывающий, есть ли у клиентского устройства сертификат Сервера администрирования. Сертификат может не существовать, например, если Агент администрирования ни разу не подключился к Серверу администрирования.

  Возможные значения:

  - `not installed` – на клиентском устройстве отсутствует сертификат Сервера администрирования.
  - `present` – клиентское устройство имеет сертификат Сервера администрирования.
- `Open UDP port` – параметр, указывающий, использует ли Агент администрирования UDP-порт для получения запросов на синхронизацию от Сервера администрирования.

  Возможные значения:

  - 0 – UDP-порт закрыт для приема запросов на синхронизацию от Сервера администрирования.
  - 1 – UDP-порт открыт для приема запросов на синхронизацию от Сервера администрирования.
- `UDP ports` – номера UDP-портов, которые может использовать Агент администрирования.
- `Location name` – сетевое местоположение устройства.
- `State of network location` – параметр, указывающий, можно ли переключить клиентское устройство с одного профиля соединений Сервера администрирования на другой.

  Возможные значения:

  - `Enabled` – профиль соединений к Серверу администрирования можно переключить для клиентского устройства.
  - `Disabled` – профиль соединений к Серверу администрирования переключить для клиентского устройства невозможно.
- `Profile to use` – профиль соединений к Серверу администрирования.
- `Condition` – IP-адрес и маска подсети сети, к которой подключено клиентское устройство.

- `Ping period, minutes` – стандартный интервал синхронизации.
- `Conn timeout, s` – время ожидания соединения.
- `RW timeout, s` – время ожидания соединения для операций чтения-записи.
- `Host ID` – идентификатор устройства в сети. `Device ID` уникален для клиентских устройств, управляемых определенным Сервером администрирования.
- `Locations of connection gateways` – параметры подключения клиентского устройства к Серверу администрирования с помощью шлюза соединения.
- `Location of distribution points` – параметры подключения клиентского устройства к Серверу администрирования с помощью точки распространения.
- `Connection with server` – параметр, указывающий, имеет ли шлюз соединения постоянное соединение с Сервером администрирования. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – шлюз соединения имеет постоянное соединение с Сервером администрирования.
  - `inactive` – шлюз соединения не имеет постоянного соединения с Сервером администрирования.
- `Connection with server through connection gateway` – параметр, указывающий, правильно ли установлено соединение с Сервером администрирования с помощью шлюза соединения. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – соединение с Сервером администрирования с помощью шлюза соединения установлено правильно.
  - `inactive` – соединение с Сервером администрирования с помощью шлюза соединения установлено некорректно.

Также вывод утилиты klnagchk может содержать одну из следующих строк:

- `Administration Server is installed on this device` – на устройстве Сервера администрирования запущена утилита klnagchk.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – утилита klnagchk запущена на устройстве, на котором установлен Агент администрирования, выполняющий роль шлюза соединения. Настроенный шлюз соединения ожидает соединения от Сервера администрирования, но Сервер администрирования не перечисляет устройство среди управляемых устройств. Вам потребуется убедиться, что Сервер администрирования инициировал соединение со шлюзом соединения.
- `This device is a connection gateway` – утилита klnagchk запускается на устройстве, которое выполняет роль шлюза соединения.
- `Acts as a distribution point` – утилита klnagchk запускается на устройстве, которое выполняет роль точки распространения.

Утилита klnagchk проверяет состояние службы Агента администрирования. Если служба не запущена, утилита останавливается. Если служба запущена, утилита отображает следующую статистику подключений:

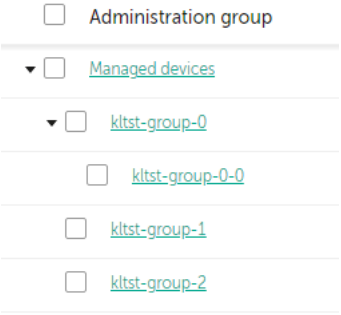
- `Ping count` – количество попыток подключения клиентского устройства к Серверу администрирования.
- `Succ. pings` – количество успешных попыток подключения клиентского устройства к Серверу администрирования.
- `Sync count` – количество попыток синхронизации параметров клиентского устройства с параметрами Сервера администрирования.
- `Succ. syncs` – количество успешных попыток синхронизации параметров клиентского устройства с Сервером администрирования.
- `Last ping` – дата и время последнего подключения.

При анализе соединения между Сервером администрирования и Агентом администрирования необходимо использовать параметры `Ping count` и `Succ. pings`. Параметры клиентского устройства синхронизируются с параметрами Сервера администрирования только в случае изменения параметров Сервера администрирования (например, при добавлении новых задач или изменении параметров политики). Иначе значения параметров `Ping count` и `Succ. pings` не изменяются.

Подробнее об устранении проблем с подключением Агента администрирования к Серверу администрирования см. Open Single Management Platform FAQ.

Создание групп администрирования

Сразу после установки Kaspersky EDR Expert в иерархии групп администрирования присутствует только одна группа администрирования – **Управляемые устройства**. При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы (см. рисунок ниже).



Просмотр иерархии групп администрирования

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.

3. Нажмите на кнопку **Добавить**.

4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.

В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Чтобы создать структуру групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Правила перемещения устройств

Рекомендуется автоматизировать процесс размещения устройств в группах администрирования при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky EDR Expert в явном виде, в разделе **Управление активами** → **Правила перемещения**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает нераспределенные устройства только один раз. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу нераспределенных устройств. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования** заблокирован в свойствах автоматически созданных правил перемещения. Такие правила создаются при добавлении задачи *Удаленная установка приложения* или создании автономного инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky EDR Expert (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

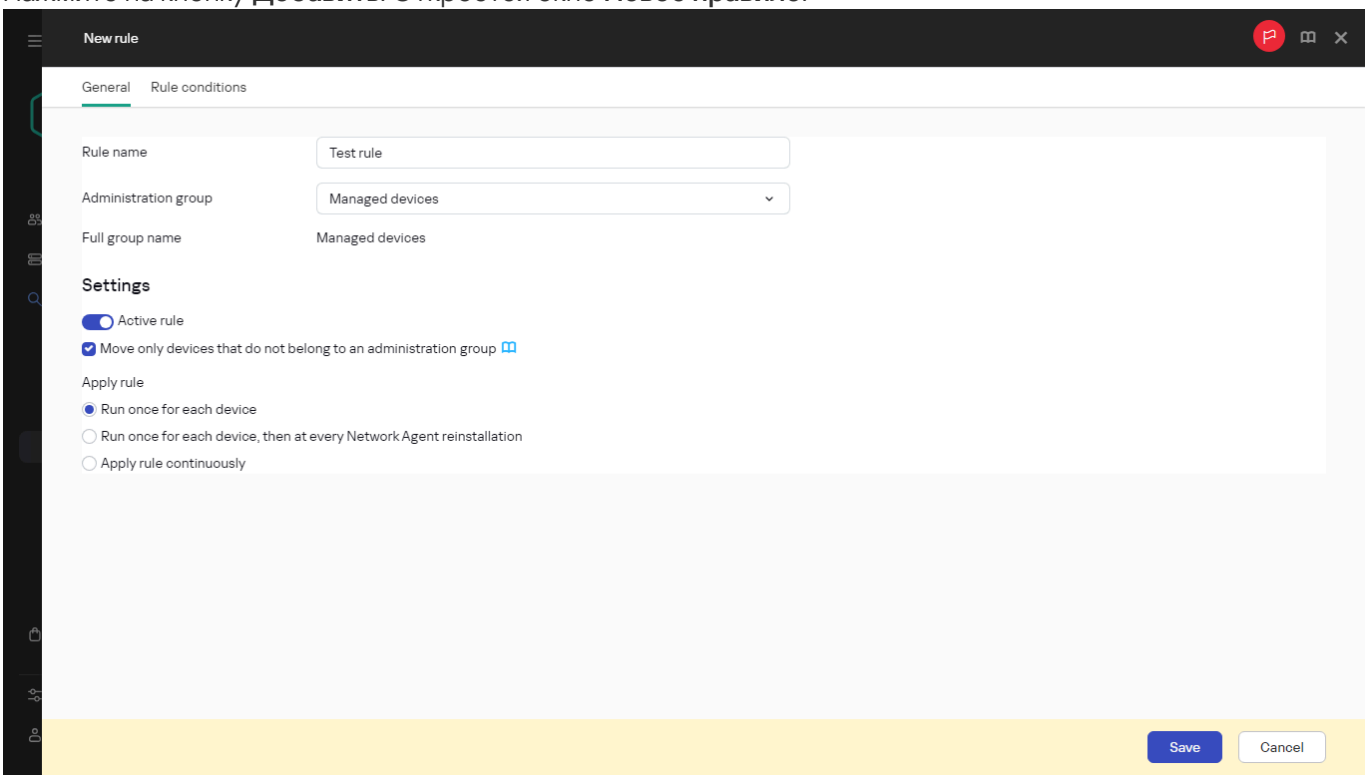
Создание правил перемещения устройств

Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Правила перемещения**.

2. Нажмите на кнопку **Добавить**. Откроется окно **Новое правило**.



Создание правила перемещения

3. В открывшемся окне укажите следующие данные на вкладке **Общие**:

- **Имя правила**

  Укажите имя нового правила активации.

  Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Приоритет**

  Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

  Если приоритет не назначен, правилу назначается самый низкий приоритет.

  При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

4. На вкладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.

5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет.

Чтобы изменить приоритет правила перемещения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Правила перемещения**.

2. В списке правил перемещения установите флажок рядом с правилом перемещения, для которого вы хотите изменить приоритет.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Изменить приоритет** и в открывшемся окне укажите новый приоритет.

   - Переместите правило вверх или вниз по списку с помощью кнопок **Вверх** или **Вниз**.

4. Нажмите на кнопку **Сохранить**.

Если выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Управление активами** → **Правила перемещения**.
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Правила перемещения**.

   Отобразится список правил перемещения устройств.

2. Установите флажок напротив правила, которое требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:

   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

   - **Активное правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

   - **Приоритет**

     Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

     Если приоритет не назначен, правилу назначается самый низкий приоритет.

     При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

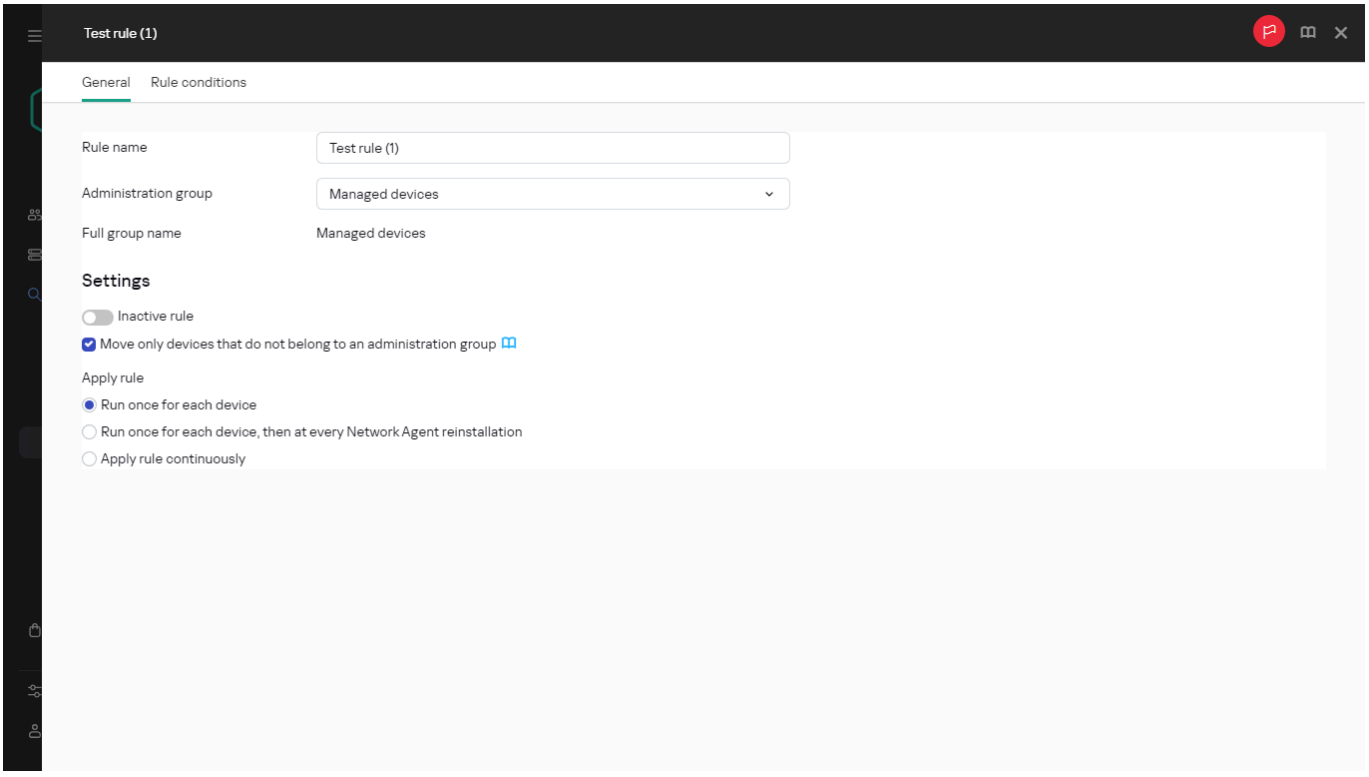
    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).



Свойства правила перемещения устройства

5. На вкладке **Условия правила** укажите критерии для устройств, которые требуется переместить автоматически.

6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

При создании или копировании правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств. Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Владелец устройства, его роль и членство в группе безопасности.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Подразделения контроллеров домена.
- Облачные сегменты.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств. Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

Применить к устройствам без выбранных тегов

Если этот параметр включен, все устройства с указанными тегами исключаются из правила перемещения устройств. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

По умолчанию параметр выключен.

Применить, если есть хотя бы один из выбранных тегов

Если этот параметр включен, правило перемещения устройств применяется к клиентским устройствам хотя бы с одним из выбранных тегов. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

По умолчанию параметр выключен.

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

Имя устройства в сети Windows

Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

Windows-домен

Правило перемещения устройств применяется ко всем устройствам, включенным в указанный Windows-домен.

DNS-имя устройства

DNS-имя домена клиентского устройства, которое вы хотите переместить. Заполните это поле, если в вашей сети есть DNS-сервер.

> Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правило перемещения устройств не будет работать.

DNS-домен

Правило перемещения устройств применяется ко всем устройствам, включенным в указанный основной DNS-суффикс. Заполните это поле, если в вашей сети есть DNS-сервер.

IP-диапазон

Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию параметр выключен.

IP-адрес подключения к Серверу администрирования

Если этот параметр включен, можно задать IP-адреса, по которым клиентские устройства подключаются к Серверу администрирования. Для этого укажите IP-диапазон, включающий все необходимые IP-адреса.

По умолчанию параметр выключен.

Устройство находится в подгруппе группы "Домены"

Если этот параметр включен, можно выбрать подгруппу группы "Домены". Соответствующие устройства должны быть расположены в выбранной подгруппе.

По умолчанию параметр выключен.

Устройство находится в IP-диапазоне

Если этот параметр включен, вы можете выбрать IP-диапазон, который вы ранее добавили в разделе **IP-диапазоны**. Соответствующие устройства должны быть включены в выбранный IP-диапазон.

По умолчанию параметр выключен.

Изменение профиля подключения

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам с измененным профилем подключения.
- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, профиль подключения которых не изменялся.
- **Значение не выбрано**. Условие не применяется.

Под управлением другого Сервера администрирования

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
- **Значение не выбрано**. Условие не применяется.

Вкладка Владелец устройства

На этой вкладке вы можете настроить правило перемещения устройств в зависимости от владельца устройств, членства в группе безопасности и ролей:

Владелец устройства

Выберите имя пользователя владельца устройства из внутренней группы безопасности. Узнайте больше о пользователях и ролях пользователей в этом разделе.

> В качестве владельца устройства может быть зарегистрировано не более одного пользователя.

Членство владельца устройства в группе безопасности Active Directory

Выберите внешнюю группу безопасности Active Directory, к которой принадлежит владелец устройства.

> Пользователь может быть частью группы безопасности Active Directory или частью группы, которая входит в эту группу безопасности Active Directory.

Роль владельца устройства

Выберите роль, назначенную владельцу устройства. Подробнее о ролях пользователей см. в этой статье.

Членство владельца устройства во внутренней группе безопасности

Выберите внутреннюю группу безопасности, к которой принадлежит владелец устройства.

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений и операционных систем, установленных на клиентских устройствах:

Агент администрирования установлен

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам, на которых установлен Агент администрирования.
- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, на которых не установлен Агент администрирования.
- **Значение не выбрано**. Условие не применяется.

Приложения

Укажите, какие управляемые приложения должны быть установлены на клиентских устройствах, чтобы к этим устройствам применялось правило перемещения устройств. Например, вы можете выбрать **Агент администрирования Kaspersky Security Center 16.3** или **Сервер администрирования Kaspersky Security Center 16.3**.

Если вы не выберете управляемое приложение, условие не будет применяться.

Версия ОС

Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

Архитектура ОС

Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

- **Нет данных**
- **x86**
- **AMD64**
- **IA64**

Чтобы проверить разрядность операционной системы клиентских устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Нажмите на значок параметров (⚙) справа.
3. Выберите параметр **Архитектура ОС** и нажмите на кнопку **Сохранить**.

   После этого для каждого управляемого устройства отобразится разрядность операционной системы.

ОС менеджера пакетов

Клиентские устройства можно выбирать по менеджеру пакетов операционной системы. В поле **ОС менеджера пакетов** можно выбрать одно из следующих значений:

- rpm – для устройств под управлением операционных систем Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux;
- apt (dpkg) – для устройств под управлением операционных систем Debian, Ubuntu, Kali;
- pkg – для устройств под управлением операционных систем FreeBSD, OpenBSD.

Чтобы проверить какой менеджер пакетов используется в операционной системе клиентских устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
3. Выберите пункт **ОС менеджера пакетов**, затем нажмите на кнопку **Сохранить**.

Для каждого управляемого устройства отображается менеджер пакетов, используемый в его операционной системе.

Версия пакета обновления ОС

В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Пользовательский сертификат

Выберите одно из следующих значений:

- **Установлено**. Правило перемещения устройств применяется только к мобильным устройствам с мобильным сертификатом.
- **Не установлено**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
- **Значение не выбрано**. Условие не применяется.

Сборка ОС

Этот параметр применим только для операционных систем Windows.

Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

Номер выпуска ОС

Этот параметр применим только для операционных систем Windows.

Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

Является виртуальной машиной

В раскрывающемся списке можно выбрать одно из следующих значений:

- **Неизвестно**. Условие не применяется.
- **Нет**. Перемещаемые устройства не должны являться виртуальными машинами.
- **Да**. Перемещаемые устройства должны являться виртуальными машинами.

Тип виртуальной машины

Часть Virtual Desktop Infrastructure

В раскрывающемся списке можно выбрать одно из следующих значений:

- **Неизвестно**. Условие не применяется.
- **Нет**. Перемещаемые устройства не должны являться частью VDI.
- **Да**. Перемещаемые устройства должны являться частью VDI.

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

Устройство входит в следующее подразделение

Если этот параметр включен, правило перемещения устройств применяется к устройствам из организационного подразделения контроллера домена, указанного в списке под параметром.

По умолчанию параметр выключен.

Включать дочерние подразделения

Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы контроллера домена.

По умолчанию параметр выключен.

Перемещать устройства из дочерних подразделений в соответствующие подгруппы

Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств

Удалять подгруппы, отсутствующие в домене

Устройство включено в следующую группу безопасности домена

Если этот параметр включен, правило перемещения устройств применяется к устройствам из доменной группы безопасности, указанной в списке под параметром.

По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в облачный сегмент. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

Устройство находится в облачном сегменте

При выборе этого параметра правило перемещения устройств применяется к клиентским устройствам, принадлежащим облачному сегменту. Вы можете выбрать нужный облачный сегмент вплоть до подсети в списке под параметром.

По умолчанию параметр выключен.

Включать дочерние объекты

Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанного облачного сегмента.

По умолчанию параметр выключен.

Перемещать устройства в соответствующие подгруппы

Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств

Удалять подгруппы, для которых нет соответствия в облачных сегментах

Устройство обнаружено с помощью API

В раскрывающемся списке можно выбрать одно из следующих значений:

- Значение не выбрано. Условие не применяется.
- **Нет**. Перемещаемые устройства, которые не были обнаружены с помощью API.
- **AWS**. Перемещаемые устройства обнаруженные с помощью AWS API.
- **Azure**. Перемещаемые устройства обнаруженные с помощью Azure API.
- **Google Cloud**. Перемещаемые устройства обнаруженные с помощью Google Cloud API.

После этого, в зависимости от выбранного значения, вы можете заполнить следующие поля:

- **Подсеть облачного устройства**.
- **Зона доступности облачного устройства**.
- **Группа размещения облачного устройства**.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

2. Выберите группу администрирования, в которую вы хотите добавить устройства:

   - Для корневой группы:

     В этом случае вы можете перейти к следующему шагу.

   - Для подгруппы:

     a. Нажмите на кнопку **Показать иерархию** в верхней части страницы.

     Название кнопки изменится на **Скрыть иерархию**.

     b. В открывшемся окне нажмите на имя подгруппы.

   Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

3. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.

4. Составьте список устройств, которые вы хотите добавить в группу администрирования.

   > В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Выберите, как вы хотите добавить устройства в список:

   - Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:

     - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.

     - Укажите IP-адреса устройств или IP-диапазон.

       > IP-диапазон не должен содержать более 1 048 576 адресов.

- Укажите DNS-имя устройства.

  Поле с именем устройства не должно содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Нажмите на кнопку **Импортировать устройства из файла**, чтобы импортировать список устройств из файла формата TXT. Каждый адрес устройства (или имя устройства) должен располагаться в отдельной строке.

  Файл не должен содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

5. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.

6. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

Также можно перемещать кластеры или массивы серверов из одной группы администрирования в другую. При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

Чтобы переместить одно или несколько устройств или кластеров в состав выбранной группы администрирования:

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:

   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** и выберите нужную группу администрирования.

     - Для корневой группы вы можете перейти к следующему шагу.

     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне выберите нужную группу администрирования.

   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Активы (Устройства)** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.

3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.

4. Нажмите на кнопку **Переместить в группу**.

5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

О кластерах и массивах серверов

Kaspersky EDR Expert поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Активы (Устройства)** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера невозможно. Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Посмотреть свойства.

- Переместить кластер или массив серверов в другую группу администрирования.

  При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.

- Удалить.

  Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Open Single Management Platform автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

Свойства кластеров или массивов серверов

Чтобы просмотреть параметры кластера или массива серверов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

Имя

Описание

Windows-домен

Windows-домен или рабочая группа, содержащая кластер или массив серверов.

NetBIOS-имя

Имя кластера или массива серверов в сети Windows.

DNS-имя

Имя DNS-домена кластера или массива серверов.

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к приложению безопасности "Лаборатории Касперского", установленного на узлах кластера. Open Single Management Platform получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства.

Приложения "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к приложению безопасности "Лаборатории Касперского", установленному на узлах кластера.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky EDR Expert выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*.

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.

- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.

- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

Число специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Число специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–100	1
Более 100	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–30	1

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
31–300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky EDR Expert будет сам выбирать, какие устройства назначать точками распространения.

Устройства с операционной системой Microsoft Windows на Arm не могут выступать в роли точек распространения.

Чтобы назначить точки распространения автоматически:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

   В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение точек распространения вручную

Kaspersky EDR Expert позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky EDR Expert будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию точек распространения.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Устройства с операционной системой Microsoft Windows на Arm не могут выступать в роли точек распространения.

Чтобы вручную назначить устройство точкой распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. Нажмите на кнопку **Назначить**.

5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

7. Нажмите на кнопку **OK**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.

9. В окне свойств настройте параметры точки распространения:

   - В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.

     - **SSL-порт**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.

     - **Включено**

       Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

Многоадресная IP-рассылка уменьшает время, необходимое для установки приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения на одно клиентское устройство.

- **Адрес IP-рассылки**

  IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

  По умолчанию Kaspersky EDR Expert автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

- **Номер порта IP-рассылки**

  Номер порта многоадресной рассылки.

  Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**

  Сетевой адрес, через который удаленные устройства подключаются к точке распространения.

- **Распространять обновления**

  Обновления распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок обновлений и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Распространять инсталляционные пакеты**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Запустить push-сервер**

  В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

- **Порт push-сервера**

  Номер порта push-сервера. Вы можете указать номер любого свободного порта.

- В разделе **Область действия** укажите группы администрирования, которым точка распространения будет распространять обновления.

- В разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения:

  - **Источник обновлений**

    Выберите источник обновлений для точки распространения:

    - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.

    - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.

      - Если такая задача уже существует для устройства, выберите задачу в списке.

      - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  - **Скачать файлы различий**

    Этот параметр включает функцию загрузки файлов различий.

    По умолчанию параметр включен.

- Если ваши точки распространения используют прокси-сервер для подключения к интернету, в подразделе **Параметры подключения к интернету** вы можете указать следующие параметры:

  - **Использовать прокси-сервер**

    Если этот флажок установлен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете. Вы можете настроить подключение к прокси-серверу в полях ввода.

    По умолчанию флажок снят.

  - **Адрес прокси-сервера**

    Адрес прокси-сервера.

  - **Номер порта**

    Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

  - **Пересылать KSN запрос Серверу администрирования**

    Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

    По умолчанию параметр включен.

  - **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

    Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  - **Игнорировать параметры прокси-сервера для подключения к KPSN**

    Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

  Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер UDP-порта. По умолчанию параметр включен.

- **UDP-порт**

  Номер UDP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Использовать HTTPS**

  Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- **HTTPS-порт**

  Номер HTTPS-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- В разделе **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:

  - **Шлюз соединения**

    Если прямое соединение между Сервером администрирования и Агентами администрирования не может быть установлено из-за организации вашей сети, вы можете использовать точку распространения в качестве шлюза соединения между Сервером администрирования и Агентами администрирования.

    Включите этот параметр, если требуется, чтобы точка распространения выполняла роль шлюза соединения между Агентами администрирования и Сервером администрирования. По умолчанию параметр выключен.

  - **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**

    Если Сервер администрирования находится за пределами демилитаризованной зоны (DMZ), в локальной сети, Агенты администрирования, установленные на удаленных устройствах, не могут подключаться к Серверу администрирования. Вы можете использовать точку распространения в качестве шлюза соединения с обратным подключением (Сервер администрирования устанавливает соединение с точкой распространения).

    Включите этот параметр, если требуется подключить Сервер администрирования к шлюзу соединения в демилитаризованной зоне.

- **Открыть локальный порт для Kaspersky Security Center Web Console**

  Включите этот параметр, если вам нужен шлюз соединения в демилитаризованной зоне, чтобы открыть порт для Web Console, находящейся в демилитаризованной зоне или в интернете. Укажите номер порта, который будет использоваться для подключения Web Console к точке распространения. По умолчанию установлен порт 13299.

  Это параметр доступен, если включен параметр **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**.

При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

- **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

  Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

- **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

  Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

  - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.

  - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

    Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос сети Windows с помощью точки распространения с операционной системой Windows.

  - **Windows-домены;**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.

- Настройте опрос контроллеров домена с помощью точки распространения.

  - **Опрос контроллеров домена**

    Вы можете включить обнаружение устройств для контроллеров домена.

Когда переключатель установлен в положение **Включено**, в поле **Опрос** вы можете выбрать контроллеры домена для опроса, а также указать для них расписание опроса.

Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллера домена. Также вы можете указать тип домена для опроса: Active Directory или Samba, FreeIPA, ALD Pro.

Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

- **Опросить текущий домен**
- **Опросить весь лес доменов**
- **Опросить указанные домены**

- Настройте опрос IP-диапазонов точкой распространения.

  - **Опрос IP-диапазонов.**

    Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

    Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

    Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.

  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

2. Выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения, нажмите на кнопку **Показать иерархию** в верхней части страницы, а затем в открывшемся окне нажмите на имя нужной группы.

   Для этого используйте пункт меню **Точки распространения**.

   Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, в этом пути нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна.

3. В главном окне приложения перейдите в раздел **Управление активами** → **Точки распространения**.

4. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить**.

5. Чтобы удалить назначенные точки распространения, выберите устройства из списка и нажмите на кнопку **Отменить назначение**.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

Включение push-сервера

В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Чтобы включить push-сервер на точке распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.

4. В разделе **Общие** включите параметр **Включено**.

5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.

6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.

7. Нажмите на кнопку **OK**.

Push-сервер включен на выбранной точке распространения.

О статусах устройства

Kaspersky EDR Expert присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky EDR Expert учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky EDR Expert не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.
- *Предупреждение* или *Предупреждение/Видим в сети*.
- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.

Условие	Описание условия	Доступные значения
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Время, прошедшее с момента перезапуска	Устройство видимо в сети, но перезапуск требуется приложением уже дольше указанного интервала времени.	Более чем 0 минут.
Причина перезапуска	Устройство видимо в сети, но приложению требуется перезагрузка устройства по одной из выбранных причин.	• Неизвестная причина • Приложение неработоспособно до перезагрузки • Для завершения обновления требуется перезагрузка; приложение работоспособно • Для инициации обновления требуется перезагрузка • Для завершения проверки или лечения требуется перезагрузка • Требуется перезагрузка для завершения удаленной установки или удаления • Завершение шифрования данных на диске
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Менее чем 0 дней.

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Kaspersky EDR Expert позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3** дней клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Когда Kaspersky EDR Expert присваивает устройству статус, для некоторых условий (см. столбец "Описание условий" в таблице выше) учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:

   - Выберите имя группы администрирования.

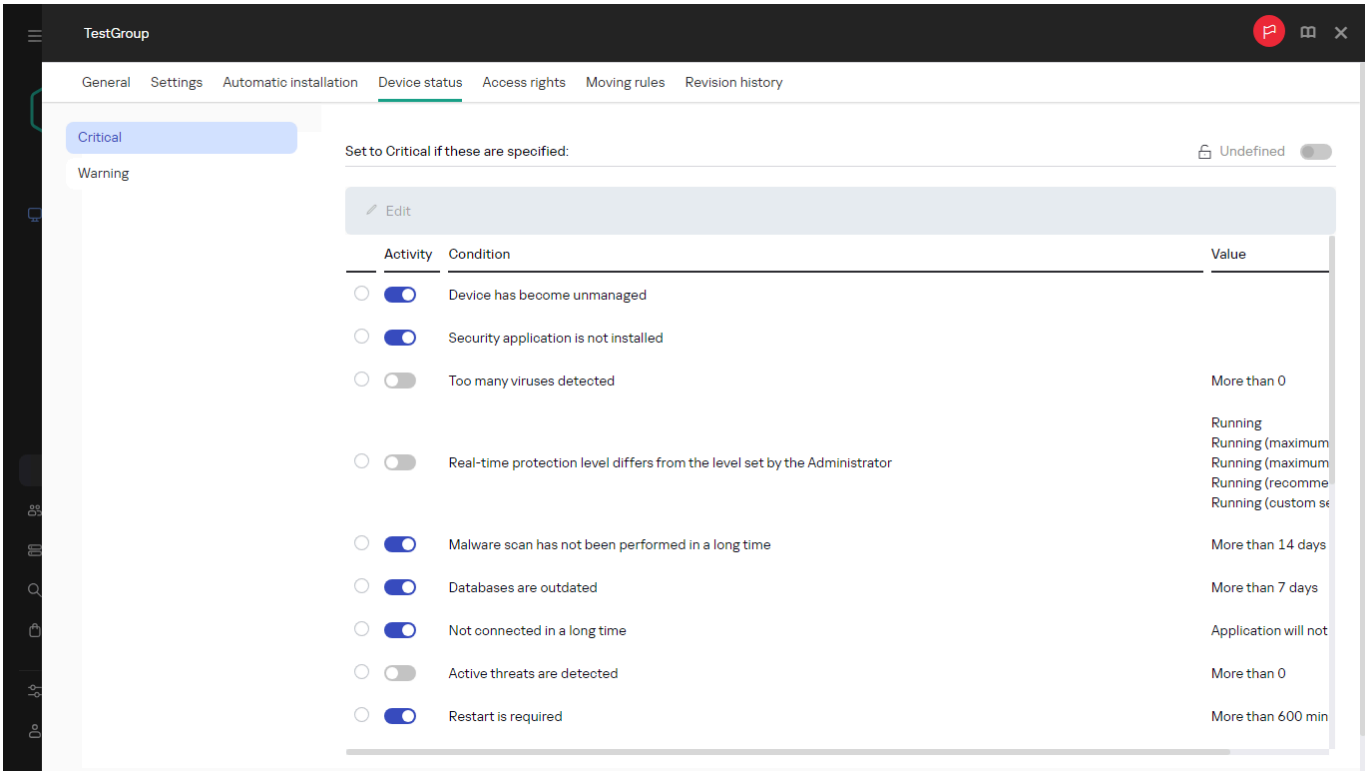
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.

3. В окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Критический**.

5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



> Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.

3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Предупреждение**.

5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Open Single Management Platform предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Open Single Management Platform позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств** или в раздел **Обнаружение устройств и развертывание** → **Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:

   - Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.

   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица устройств.

Также вы можете запускать задачи для устройств выборки. Для этого выберите одно или несколько устройств, затем нажмите на кнопку **Запустить задачу** и выберите: **Создать задачу**, которая будет применена к этим устройствам, либо **Применить существующую задачу**.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.

3. Введите имя новой выборки.

4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:

   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.

   - **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.

   - **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

   Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.

5. Нажмите на кнопку **Добавить**.

6. В открывшемся окне укажите условия, которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **Сохранить**.

7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

Чтобы настроить параметры выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.

3. На вкладке **Общие** перейдите по ссылке **Новое условие**.

4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.

5. Нажмите на кнопку **Сохранить**.

   Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

По умолчанию параметр выключен.

Если вы включите этот параметр, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

В следующем примере показана логика работы инверсии:

- **Условие**: на вашем устройстве установлена операционная система с типом Linux и номером сборки 00.0.000.

- **Инвертированное состояние**: на вашем устройстве установлена операционная система с НЕ (тип Linux и номер сборки 00.0.000), что эквивалентно следующему:

  Есть операционная система с типом НЕ Linux ИЛИ с номером сборки НЕ 00.0.000.

Таким образом, выборка будет включать устройства с операционной системой, например, с типом Windows и номером сборки 00.0.000 или типом Linux и любым номером сборки, отличным от 00.0.000.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

Имя устройства

Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

Домен

Отображаются все устройства, входящие в указанную рабочую группу.

Группа администрирования

Будут отображаться устройства, входящие в указанную группу администрирования.

Описание

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

Для описания текста в поле **Описание** допустимо использовать следующие символы:

- Внутри одного слова:

  - *****. Заменяет любую строку длиной 0 и более символов.

  Пример:

  Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

  - **?.** Заменяет любой один символ.

  Пример:

  Для описания таких фраз, как **SUSE Linux корпоративный сервер 12** или же **SUSE Linux корпоративный сервер 15**, можно ввести **SUSE Linux Enterprise Server 1?**.

  Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

- Для связи нескольких слов:

  - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

  Пример:

  Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

  - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

  Пример:

  Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

  - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

  Пример:

  Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

  - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

  Пример:

  Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

IP-диапазон

Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию параметр выключен.

Под управлением другого Сервера администрирования

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.

- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.

- **Значение не выбрано**. Условие не применяется.

В разделе **Контроллеры домена** можно настроить критерии включения устройств в выборку по членству в домене:

Устройство в подразделении домена

Если этот параметр включен, в выборку будут включаться устройства из подразделения домена, указанного в поле ввода.

По умолчанию параметр выключен.

Это устройство является членом группы безопасности домена

Если этот параметр включен, в выборку будут включаться устройства из группы безопасности домена, указанной в поле ввода.

По умолчанию параметр выключен.

В разделе **Действия в сети** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

Является точкой распространения

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут включены устройства, являющиеся точками распространения.
- **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

Не разрывать соединение с Сервером администрирования

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен**. Выборка будет включать устройства, для которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен**. Выборка будет включать устройства, для которых снят флажок **Не разрывать соединение с Сервером администрирования**.
- **Значение не выбрано**. Критерий не применяется.

Переключение профиля подключения

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано**. Критерий не применяется.

Последнее подключение к Серверу администрирования

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

Новые устройства, обнаруженные при опросе сети

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если этот параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

По умолчанию параметр выключен.

Устройство в сети

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет**. Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано**. Критерий не применяется.

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

Статус устройства

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *OK*, *Критический* или *Предупреждение*.

Статус постоянной защиты

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Device status description

В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK, Критический* или *Предупреждение*.

В разделе **Статусы компонентов управляемых приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

Статус защиты данных от утечек

Поиск устройств по статусу компонента защиты от утечки данных (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

Статус защиты для серверов совместной работы

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлена*, *Запускается, Приостановлена*, *Выполняется*, *Сбой*).

Статус антивирусной защиты почтовых серверов

Поиск устройств по статусу защиты почтовых серверов (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

Статус Endpoint Sensor

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **ОС** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

Тип платформы

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

Версия пакета обновления ОС

В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Архитектура ОС

В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

Сборка ОС

> Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

Номер выпуска ОС

> Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

Является виртуальной машиной

В раскрывающемся списке можно выбрать следующие элементы:

- **Не определено**.
- **Нет**. Искомые устройства не должны являться виртуальными машинами.
- **Да**. Искомые устройства должны являться виртуальными машинами.

Тип виртуальной машины

В раскрывающемся списке можно выбрать производителя виртуальной машины.

Этот список доступен, если в раскрывающемся списке **Является виртуальной машиной** выбрано значение **Да** или **Неважно**.

Часть Virtual Desktop Infrastructure

В раскрывающемся списке можно выбрать следующие элементы:

- **Не определено**.
- **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
- **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

> Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Устройство

В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

В поле поддерживается полнотекстовый поиск.

Поставщик

В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

В поле поддерживается полнотекстовый поиск.

Имя устройства

Устройство с указанным именем будет включено в выборку.

Описание

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

Поставщик устройства

Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

Название производителя можно ввести в окне свойств устройства.

Серийный номер

Оборудование с серийным номером, указанным в поле, будет включено в выборку.

Инвентарный номер

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

Пользователь

Оборудование пользователя, указанного в поле, будет включено в выборку.

Расположение

Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

Частота процессора (МГц) от

Минимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

Частота процессора (МГц) до

Максимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

Количество виртуальных ядер процессора от

Минимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

Количество виртуальных ядер процессора до

Максимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

Объем жесткого диска (ГБ), от

Минимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Объем жесткого диска (ГБ), до

Максимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Объем оперативной памяти (МБ) от

Минимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Объем оперативной памяти (МБ) до

Максимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Информация о приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

Название приложения

Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

Версия приложения

Поле ввода, в котором указывается версия выбранного приложения.

Поставщик

Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

Статус приложения

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

Искать по обновлению

Если этот параметр включен, поиск будет выполняться по данным об обновлении приложений, установленных на искомых устройствах. После установки этого флажка вместо полей **Название приложения**, **Версия приложения** и **Статус приложения** будут отображаться поля **Имя обновления**, **Версия обновления** и **Статус** соответственно.

По умолчанию параметр выключен.

Название несовместимого приложения безопасности

Раскрывающийся список, в котором можно выбрать приложения безопасности сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

Тег приложения

В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

Применить к устройствам без выбранных тегов

Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если этот параметр выключен, критерий не применяется.

По умолчанию параметр выключен.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.

- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Информация о приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

Название приложения

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

Версия приложения

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

Название критического обновления

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

Статус приложения

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

Выбор периода последнего обновления модулей

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

Устройство находится под управлением Сервера администрирования

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky EDR Expert:

- **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky EDR Expert.
- **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky EDR Expert.
- **Значение не выбрано**. Критерий не применяется.

Приложение безопасности установлено

В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение безопасности:

- **Да**. Приложение включает в выборку устройства, на которых установлено приложение безопасности.
- **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение безопасности.
- **Значение не выбрано**. Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

Дата выпуска баз

Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

По умолчанию параметр выключен.

Количество записей в базах

Если этот параметр включен, поиск клиентских устройств выполняется по количеству записей в базе. В полях ввода можно задать нижнее и верхнее значения количества записей антивирусной базы.

По умолчанию параметр выключен.

Последняя проверка

Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

По умолчанию параметр выключен.

Обнаружены угрозы

Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию параметр выключен.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

> Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в OSMP Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

Статус

Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства, Остановлен*, *Приостановлено*, *Запускается*, *Выполняется, Сбой*, *Не установлен, Не поддерживается лицензией*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные приложениями:

- *Остановлено* – компонент отключен и в данный момент не работает.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.
- *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

Версия

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

Применить, если есть хотя бы один из выбранных тегов

Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию параметр выключен.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

Все устройства, имеющие этот тег

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

Все устройства, не имеющие этого тега

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

Последний пользователь, выполнивший вход в систему

Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся выбранным пользователем.

Пользователь, уже выполнявший вход в систему

Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Владелец устройства

В разделе **Владелец устройства** вы можете настроить критерии включения устройств в выборку в соответствии с зарегистрированными владельцами устройства, их ролями и их членством в группах безопасности:

Владелец устройства

Выберите имя пользователя владельца устройства из внутренней группы безопасности. Узнайте больше о пользователях и ролях пользователей в этом разделе.

В качестве владельца устройства может быть зарегистрировано не более одного пользователя.

Членство владельца устройства в группе безопасности Active Directory

Выберите внешнюю группу безопасности Active Directory, к которой принадлежит владелец устройства.

Пользователь может быть частью группы безопасности Active Directory или частью группы, которая входит в эту группу безопасности Active Directory.

Роль владельца устройства

Выберите роль, назначенную владельцу устройства. Подробнее о ролях пользователей см. в этой статье.

Членство владельца устройства во внутренней группе безопасности

Выберите внутреннюю группу безопасности, к которой принадлежит владелец устройства.

Экспорт списка устройств из выборки устройств

Open Single Management Platform позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.
3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Теги устройств

В этом разделе описаны теги устройств, приведены инструкции по их созданию и изменению, а также по назначению тегов устройствам вручную и автоматически.

Теги устройств

Open Single Management Platform позволяет назначать *теги* устройствам. Тег представляет собой строковое значение, которое можно использовать для группировки, описания или поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Если вы хотите отметить отдельное устройство, вы можете назначить тег вручную. Автоматическое назначение тегов выполняется Open Single Management Platform одним из следующих способов:

- В соответствии с указанными правилами назначения тегов.

- В соответствии с указанным приложением.

Не рекомендуется использовать разные способы назначения тегов для назначения одного и того же тега. Например, если тег назначается правилом, не рекомендуется назначать этот тег устройствам вручную.

Если теги назначаются правилами, устройствам назначаются теги автоматически при соблюдении указанных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы CentOS, назначается тег `[CentOS]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства под управлением операционной системы CentOS и назначить им задачу.

> Вы можете добавить только одно правило автоматического назначения тегов для каждого тега. Если вы создадите еще одно правило для того же тега, предыдущее правило будет заменено.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

Создание тегов устройств

Чтобы создать тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. На вкладке **Теги устройств** нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. На вкладке **Теги устройств** выделите тег, который требуется переименовать.

   Откроется окно свойств тега.

3. В поле **Тег** измените название тега.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Вы можете удалить только теги, назначенные вручную.

Чтобы удалить тег устройства, назначенный вручную:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.

   Отобразится список тегов.

2. На вкладке **Теги устройств** выберите теги устройства, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **Да**.

   Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

При удалении тега, назначенного устройству автоматически, правило не удаляется, и тег будет назначен новому устройству, когда устройство впервые соответствует условиям правила. Если вы удалите правило автоматического назначения тега, указанный в условиях правила, будет удален со всех устройств, которым он был назначен, но не будет удален из списка тегов. При необходимости вы можете вручную удалить тег из списка.

Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Для того чтобы управлять такими тегами, используйте утилиту klscflag.

Просмотр устройств, которым назначен тег

Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.

2. На вкладке **Теги устройств** перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Вы будете перенаправлены в раздел **Активы (Устройства)** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.

3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам. В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

   Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег.

В панели инструментов можно выполнить следующие действия:

- Назначить устройству другой тег.
- Удалить уже назначенный тег.
- Просмотреть все теги устройств, которые существуют на Сервере администрирования.

Вы не можете просматривать назначенные теги локально на устройстве.

Назначение тегов устройству вручную

Чтобы вручную назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
   - Чтобы создать и назначить новый тег, выберите пункт **Создать тег** и укажите тег.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **OK**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Выбранный тег будет назначен устройству.

Удаление назначенного тега с устройства

Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.
5. В верхней части списка нажмите на кнопку **Отменить назначение тега**.
6. В появившемся окне нажмите на кнопку **OK**.

   Тег будет снят с устройства.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Для того чтобы управлять этими тегами, используйте утилиту klscflag.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств** → **Правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, а затем нажмите на кнопку **Настроить правила автоматического назначения тегов**.

Отобразится список правил автоматического назначения тегов устройствам.

Изменение правил автоматического назначения тегов устройствам

Чтобы изменить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Выберите правило, которое требуется изменить.

   Откроется окно с параметрами правила.
3. Измените основные параметры правила:

   a. В поле **Имя правила** измените название правила.

      Название может содержать не более 256 символов.

   b. Выполните одно из следующих действий:

      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.
4. Выполните одно из следующих действий:

   - Если вы хотите добавить новое условие, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры нового условия.
   - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры.
   - Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.
5. В окне с параметрами условий нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

Создание правил автоматического назначения тегов устройствам

Чтобы создать правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами нового правила.
3. Укажите основные параметры правила:

   a. В поле **Имя правила** введите название правила.

      Название не должно быть длиннее 256 символов.

b. Выполните одно из следующих действий:

- Включите правило, установив переключатель в положение **Правило включено**.
- Выключите правило, установив переключатель в положение **Правило выключено**.

c. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

Название не должно быть длиннее 256 символов.

4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

Откроется окно с параметрами нового условия.

5. Укажите название условия.

Название не должно быть длиннее 256 символов. Название условия должно быть уникальным в рамках одного правила.

6. Настройте срабатывание правила по следующим условиям: Можно выбрать несколько условий.

- **Сеть** – сетевые свойства устройства (например, DNS-имя устройства или принадлежность устройства к IP-подсети).

> Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Приложения** – наличие на устройстве Агента администрирования, тип, версия, архитектура операционной системы и менеджер пакетов.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Реестр приложений** – наличие на устройстве приложений различных производителей.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила.
- После выполнения правила вручную.
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства.

Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

Чтобы выполнить правила автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

   Выбранные правила будут выполнены.

Удаление правил автоматического назначения тегов с устройств

Чтобы удалить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажок напротив правила, которое требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

   Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

   Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска. Также шифрование данных предотвращает доступ к данным неавторизованных пользователей и приложений.

Вы можете использовать функцию шифрования данных, если в вашей сети есть управляемые устройства с операционной системой Windows, на которых установлено приложение Kaspersky Endpoint Security for Windows. В этом случае на устройствах под управлением операционной системы Windows вы можете управлять следующими типами шифрования:

- шифрование диска BitLocker;
- шифрование диска Kaspersky.

Не рекомендуется включать шифрование в VDI.

С помощью этих компонентов Kaspersky Endpoint Security for Windows вы можете, например, включать или выключать шифрование, просматривать список зашифрованных жестких дисков, формировать и просматривать отчеты о шифровании.

Чтобы настроить шифрование, настройте политику Kaspersky Endpoint Security for Windows в Open Single Management Platform. Kaspersky Endpoint Security for Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в онлайн-справке Kaspersky Endpoint Security for Windows.

Управление шифрованием для иерархии Серверов администрирования в настоящее время недоступно в Web Console. Используйте главный Сервер администрирования для управления зашифрованными устройствами.

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса.

Просмотр списка зашифрованных жестких дисков

В Open Single Management Platform вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security for Windows отправляет в Open Single Management Platform информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

Чтобы просмотреть события шифрования управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя управляемого устройства.
3. На вкладке **Общие** перейдите в раздел **Защита**.
4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.

- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.

- Отчет о правах доступа к зашифрованным жестким дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.

- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.

- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств

- Отчет о правах доступа к зашифрованным жестким дискам

- Отчет об ошибках шифрования файлов

*Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса включен.

2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.

3. Откройте один из следующих разделов:

   - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.

   - **События шифрования** – формирует отчет об ошибках шифрования файлов.

4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в справке Kaspersky Endpoint Security для соответствующей платформы.

Порядок предоставления доступа к зашифрованному жесткому диску в автономном режиме в Kaspersky Endpoint Security for Windows:

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в онлайн-справке Kaspersky Endpoint Security for Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security for Windows.

2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

   Отобразится список зашифрованных жестких дисков.

3. Выберите диск, к которому пользователь запросил доступ.

4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

5. В открывшемся окне выберите плагин Kaspersky Endpoint Security for Windows.

6. Следуйте инструкциям, приведенным в онлайн-справке Kaspersky Endpoint Security for Windows (см. инструкции для OSMP Console в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

Передача ключей шифрования между Серверами администрирования

Если на управляемом устройстве включена функция шифрования данных, ключ шифрования хранится на Сервере администрирования. Ключ шифрования используется для доступа к зашифрованным данным и для управления политикой шифрования.

Ключ шифрования должен быть передан на другой Сервер администрирования в следующих случаях:

- Перенастройка Агента администрирования на управляемом устройстве для назначения устройства другому Серверу администрирования. Если это устройство содержит зашифрованные данные, ключ шифрования должен быть передан на целевой Сервер администрирования. В противном случае не удастся расшифровать данные.

- Шифрование съемного диска, подключенного к устройству D1, которым управляет Сервер администрирования S1, и затем подключение этого съемного диска к устройству D2, управляемому Сервером администрирования S2. Для доступа к данным на съемном диске ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

- Шифрование файла на устройстве D1, управляемом Сервером администрирования S1, и затем попытка получить доступ к файлу на устройстве D2, управляемом Сервером администрирования S2. Для доступа к файлу ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

Ключи шифрования можно передавать следующими способами:

- Автоматически, включив параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах двух Серверов администрирования, между которыми должен передаваться ключ шифрования. Если этот параметр выключен для одного из Серверов администрирования, автоматическая передача ключей шифрования невозможна.

  При включении параметра **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах Сервера администрирования, Сервер администрирования отправляет ключи шифрования на главный Сервер администрирования (если он существует) на один уровень иерархии выше.

  Когда вы пытаетесь получить доступ к зашифрованным данным, Сервер администрирования сначала ищет ключ шифрования в своем хранилище. Если включен параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**, а требуемый ключ шифрования отсутствует в хранилище, Сервер администрирования дополнительно отправляет запрос на главный Сервер администрирования (если он существует), чтобы получить требуемый ключ шифрования. Запрос отправляется на все главные Серверы администрирования, вплоть до Сервера на самом верхнем уровне иерархии.

- Вручную от одного Сервера администрирования другому путем экспорта и импорта файла, содержащего ключи шифрования.

  Экспорт и импорт ключей шифрования – это действия, включенные в функционал управления ключами шифрования. Чтобы выполнить эти действия, настройте права доступа к функции для пользователей Open Single Management Platform следующим образом:

  - Предоставить право **Чтение** к функции Управление ключами шифрования для пользователя, который экспортирует ключи шифрования с подчиненного Сервера администрирования.

  - Предоставить право **Запись** к функции Управление ключами шифрования для пользователя, импортирующего ключи шифрования на требуемый Сервер администрирования.

Чтобы включить автоматическую передачу ключей шифрования между Серверами администрирования в иерархии:

1. Перейдите в свойства нужного Сервера администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

   Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Включите параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**.

4. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Ключи шифрования будут переданы на главный Сервер администрирования (если он существует) при следующей синхронизации (пакете пульса). Этот Сервер администрирования также предоставляет по запросу ключ шифрования от своего хранилища подчиненному Серверу администрирования.

Чтобы передать ключи шифрования между Серверами администрирования вручную:

1. Перейдите в свойства Сервера администрирования, с которого вы хотите экспортировать ключи шифрования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

   Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Нажмите на кнопку **Экспорт ключей шифрования**.

   Убедитесь, что пользователю, который экспортирует ключи шифрования с Сервера, предоставлено право **Чтение** к функции Управления ключами шифрования.

4. В окне **Экспортировать ключи шифрования с Сервера администрирования?** выполните следующие действия:

   a. Укажите пароль, чтобы защитить файл от несанкционированного доступа.

   b. Укажите, куда сохранить файл.

   Запомните пароль. Утерянный пароль не может быть восстановлен. Если пароль утерян, необходимо повторить процедуру экспорта. Поэтому запишите пароль и держите его под рукой.

5. Передайте файл на другой Сервер администрирования, например, с помощью папки общего доступа или съемного диска.

6. Перейдите в свойства Сервера администрирования, на который вы хотите импортировать ключи шифрования.

7. В окне свойств выберите раздел **Алгоритм шифрования**.

8. Нажмите на кнопку **Импорт ключей шифрования**.

   Убедитесь, что пользователю, импортирующему ключи шифрования на Сервер, предоставлено право **Запись** к функции Управления ключами шифрования.

9. Выберите файл, содержащий ключи шифрования.

10. Укажите пароль и нажмите на кнопку **OK**.

Ключи шифрования будут переданы на целевой Сервер администрирования.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования на другой для конкретных клиентских устройств. Для этого используйте задачу *Смена Сервера администрирования*.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.

2. Создайте задачу обслуживания Сервера администрирования.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера создания задачи **Новая задача** выберите приложение **Kaspersky Security Center 16.3** и тип задачи **Смена Сервера администрирования**. Затем укажите устройства, для которых вы хотите сменить Сервер администрирования:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security for Windows.

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Перейдите к свойствам нужной группы администрирования одним из следующих способов:

   - Выберите имя группы администрирования.

   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.

3. В окне свойств перейдите на вкладку **Параметры**.

4. В разделе **Наследование** включите или выключите следующие параметры:

   - **Наследовать из родительской группы**

     Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

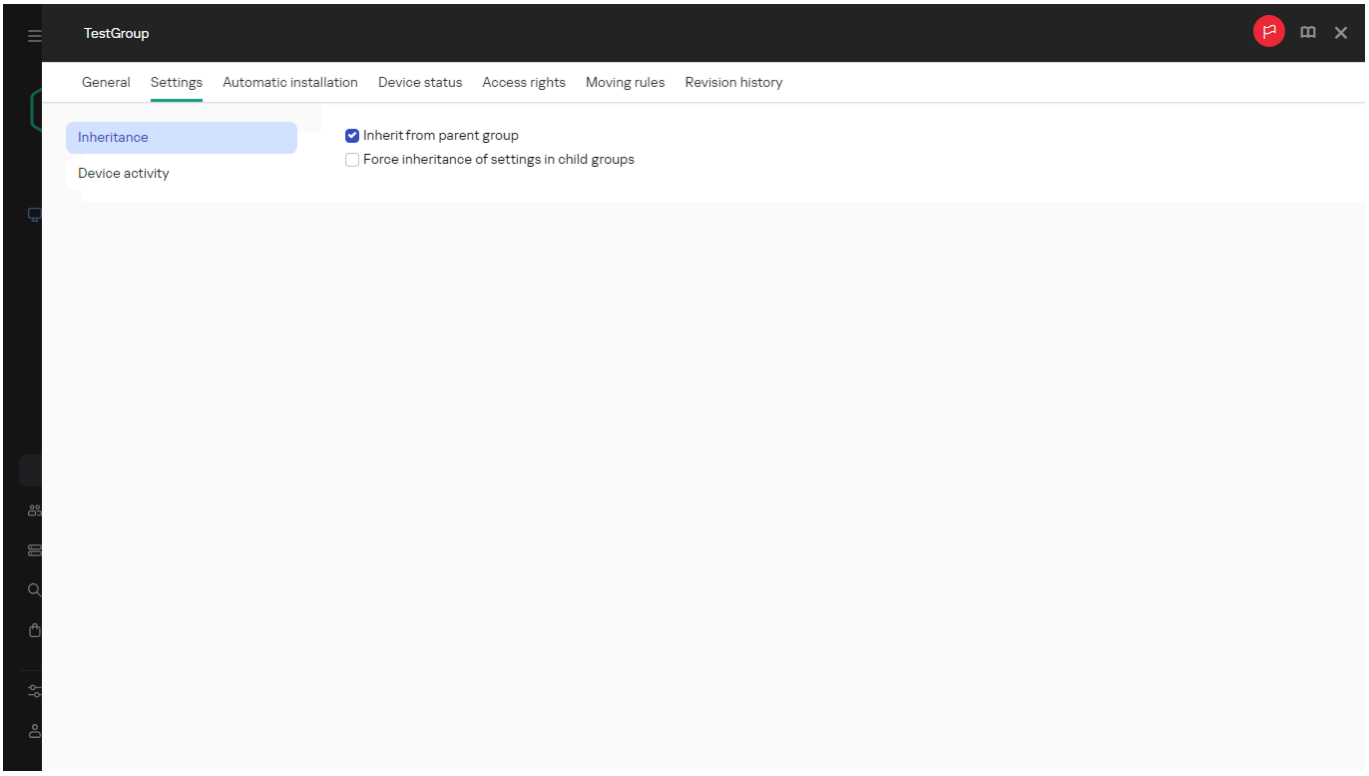
     Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

     По умолчанию параметр включен.

- **Обеспечить принудительное наследование параметров для дочерних групп**

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.



Свойства группы администрирования

5. В разделе **Активность устройств** включите или выключите следующие параметры:

- **Уведомлять администратора, если устройство неактивно больше (сут)**

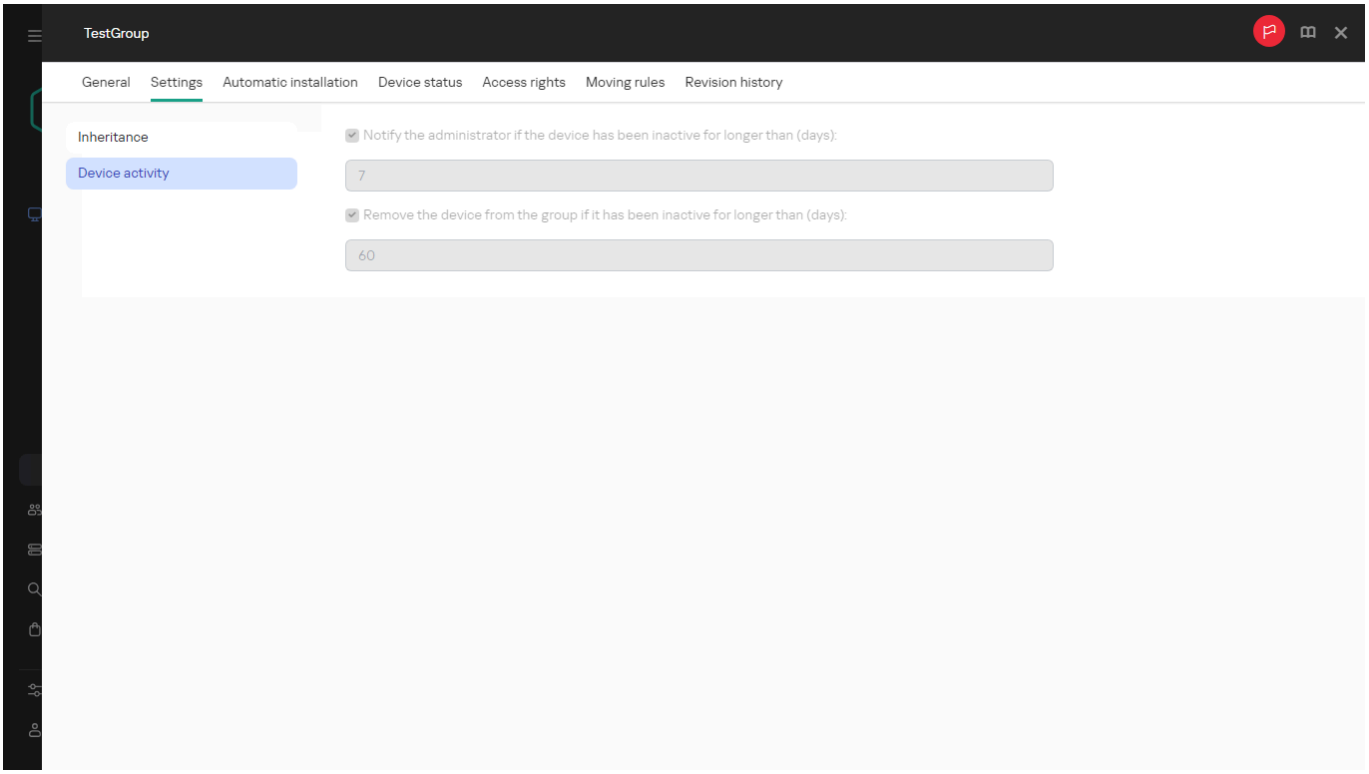
  Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

  По умолчанию параметр включен.

- **Удалять устройство из группы, если оно неактивно больше (сут)**

  Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

По умолчанию параметр включен.



Свойства группы администрирования

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

Удаленный доступ к управляемым устройствам

Open Single Management Platform позволяет устанавливать удаленное подключение к управляемым устройствам. Вы можете получить удаленный доступ к управляемому устройству с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа. После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

Способы установки удаленного подключения зависят от того, какая платформа используется на устройстве с Консолью OSMP. Консоль OSMP может быть установлена на устройство с операционной системой Windows или Linux, отличное от устройства Сервера администрирования.

От Консоли OSMP, установленной на устройстве с операционной системой Linux, вы можете установить следующие подключения:

- К управляемому устройству с операционной системой Linux с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).

- К управляемому устройству с операционной системой Windows с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).

От Консоли OSMP, установленной на устройстве с операционной системой Windows, вы можете установить следующие подключения:

- К управляемому устройству с операционной системой Linux с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).
- К управляемому устройству с операционной системой Windows с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Совместный доступ к рабочему столу (Windows Desktop Sharing, WDS).

Удаленное подключение к управляемым устройствам не поддерживается при доступе к Консоли OSMP с устройства с операционной системой Microsoft Windows на Arm.

Чтобы установить удаленное подключение с устройством, у вам потребуется следующее:

- Утилита klsctunnel.

  Утилита "Лаборатории Касперского" используется для туннелирования соединения между управляемым устройством и Сервером администрирования.

  Open Single Management Platform позволяет туннелировать TCP-соединения от Консоли OSMP через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью OSMP, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью OSMP с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

  Утилиту можно скачать, когда удаленное подключение установлено с помощью Консоли OSMP или вручную. Утилита klsctunnel установлена на устройстве Сервера администрирования.

  Утилита klsctunnel используется для всех типов удаленного подключения (RDP, VNC, WDS).

- RDP- или VNC-клиент.

  RDP- или VNC-клиент установлен на устройстве Сервера администрирования. Этот клиент позволяет вам получить удаленный доступ к управляемому устройству, используя адрес и порт для локального подключения, предоставленные утилитой klsctunnel.

RDP-подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

- Совместный доступ к рабочему столу Windows (только для управляемых устройств с операционной системой Windows)

  Эта функция позволяет вам подключиться к существующему сеансу на клиентском устройстве, не отключая пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

  При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky EDR Expert.

  Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Удаленный доступ с Linux-устройства с Консолью OSMP к управляемому Linux-устройству

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- На управляемом устройстве с операционной системой Linux установлен RDP-сервер (если вы подключаетесь к управляемому устройству с использованием Remote Desktop Connection).
- На управляемом устройстве с операционной системой Linux установлен VNC-сервер (если вы подключаетесь к управляемому устройству с использованием Virtual Network Computing).
- У администратора есть право **Запуск RDP-сеансов** для установки RDP-соединений (если вы подключаетесь к управляемому устройству с помощью Remote Desktop Connection).
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC (если вы подключаетесь к управляемому устройству с помощью Virtual Network Computing).

Чтобы подключиться к управляемому устройству с операционной системой Linux по RDP или VNC с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.

3. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   При скачивании утилиты учитывайте следующее:

   - Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

     Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

   - Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent_srv.

4. В окне **Подключиться к удаленному рабочему столу** укажите порт подключения. По умолчанию номер порта – 3389.

5. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

6. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения клиента удаленного доступа.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

7. Запустите клиент удаленного доступа (RDP или VNC) и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне клиента удаленного доступа.

Удаленный доступ с Linux-устройства с Консолью OSMP к управляемому Windows-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Удаленное подключение разрешено в параметрах операционной системы управляемого устройства.
- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.

Чтобы подключиться к управляемому устройству с операционной системой Windows по RDP с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.

2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.

3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **RDP**.

4. Если удаленное подключение не разрешено в параметрах операционной системы управляемого устройства, разрешите удаленное подключение централизованно, нажав на кнопку **Изменить параметры**.

   Если параметры применены правильно, отображается уведомление. Также на управляемом устройстве в разделе **Параметры** → **Система** → **Удаленный рабочий стол** должен быть включен параметр **Включить удаленный рабочий стол**.

   Если удаленное подключение разрешено в параметрах операционной системы управляемого устройства, кнопка **Изменить параметры** не отображается.

5. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.

6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

8. Запустите RDP-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне RDP-клиента.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Система Virtual Network Computing (VNC)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- На управляемом устройстве с операционной системой Windows установлен VNC-сервер.
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC.

Чтобы подключиться к управляемому устройству с операционной системой Windows по VNC с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **VNC**.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   При скачивании утилиты учитывайте следующее:

   - Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

     Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".
   - Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent.
5. В окне **Подключиться к удаленному рабочему столу** укажите порт VNC-подключения. По умолчанию номер порта – 5900.
6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.
7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

8. Запустите VNC-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне VNC-клиента.

Удаленный доступ с Windows-устройства с Консолью OSMP к управляемому Linux-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен RDP-сервер.
- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.

Чтобы подключиться к управляемому устройству с операционной системой Linux по RDP с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **RDP**.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.
5. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

6. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.

7. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.

8. Укажите учетные данные учетной записи, под которой вы в настоящий момент вошли в Консоль OSMP, и подключитесь к управляемому устройству.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Система Virtual Network Computing (VNC)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- На управляемом устройстве с операционной системой Linux установлен VNC-сервер.
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC.

Чтобы подключиться к управляемому устройству с операционной системой Linux по VNC с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.

3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **VNC**.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

При скачивании утилиты учитывайте следующее:

- Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

  Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

- Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent.

5. В окне **Подключиться к удаленному рабочему столу** укажите порт VNC-подключения. По умолчанию номер порта – 5900.

6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.

8. Нажмите на кнопку **Открыть порт**.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

   Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

9. Запустите VNC-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне VNC-клиента.

Удаленный доступ с Windows-устройства с Консолью OSMP к управляемому Windows-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.
- Удаленное подключение разрешено в параметрах операционной системы управляемого устройства.

Чтобы подключиться к управляемому устройству с операционной системой Windows по RDP с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **Подключение к удаленному рабочему столу**.
4. Если удаленное подключение не разрешено в параметрах операционной системы управляемого устройства, разрешите удаленное подключение централизованно, нажав на кнопку **Изменить параметры**.

   Если параметры применены правильно, отображается уведомление. Также на управляемом устройстве в разделе **Параметры** → **Система** → **Удаленный рабочий стол** должен быть включен параметр **Включить удаленный рабочий стол**.

   Если удаленное подключение разрешено в параметрах операционной системы управляемого устройства, кнопка **Изменить параметры** не отображается.
5. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.
6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.
7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.
8. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.
9. Укажите учетные данные учетной записи, под которой вы в настоящий момент вошли в Консоль OSMP, и подключитесь к управляемому устройству.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Совместный доступ к рабочему столу (Windows Desktop Sharing, WDS)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- У администратора есть право **Подключение к существующим RDP-сеансам** для установки WDS-соединения.
- Лицензия на Системное администрирование доступна.
- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

  Проверьте, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, и убедитесь, что ключ CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} есть в реестре Windows.
- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.

Чтобы подключиться к управляемому устройству с операционной системой Windows по VNC с помощью Консоли OSMP, которая открыта на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **Совместный доступ к рабочему столу Windows**.

   Если лицензия на Системное администрирование недоступна, отображается сообщение об ошибке.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

При скачивании утилиты учитывайте следующее:

- Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

  Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

- Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent.

5. В списке доступных пользовательских сеансов, активных в выбранной выборке устройств, выберите сеанс, к которому вы хотите подключиться.

   Удаленный пользователь должен разрешить подключение. Если удаленный пользователь отклоняет подключение или если удаленный пользователь не разрешает подключение в течение периода ожидания, отображается сообщение об ошибке.

6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.

8. Нажмите на кнопку **Открыть порт**.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

   Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок меню ( ) в верхнем левом углу окна и выберите **Интерактивный режим**.

Управление активами

Активы представляют собой компьютеры в организации. Вы можете добавить активы в OSMP, тогда OSMP будет автоматически добавлять идентификаторы активов при обогащении событий и при анализе событий вы получите дополнительную информацию о компьютерах в организации.

Вы можете добавить активы в OSMP следующими способами:

- Импортировать активы:
  - Из MaxPatrol VM.
  - По расписанию: из Kaspersky Security Center и KICS for Networks.

    По умолчанию импорт активов выполняется каждые 12 часов, периодичность можно настроить. Также возможен импорт активов по запросу, при этом выполнение импорта по запросу не повлияет на время импорта по расписанию. OSMP импортирует из базы Kaspersky Security Center сведения об устройствах с установленным Агентом администрирования Kaspersky Security Center, который подключался к Kaspersky Security Center, то есть поле Connection time в базе SQL – непустое. OSMP импортирует следующую информацию об устройстве: имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании и программном обеспечении, включая операционную систему, а также об уязвимостях, то есть информацию, полученную от Агентов администрирования Kaspersky Security Center.
- Создать активы вручную через веб-интерфейс или с помощью API.

  Вы можете добавить активы вручную. При этом необходимо вручную указать следующие данные: адрес, FQDN, название и версия операционной системы, аппаратные характеристики. Добавление информации об уязвимостях активов через веб-интерфейс не предусмотрено. Вы можете указать информацию об уязвимостях, если будете добавлять активы с помощью API.

Вы можете управлять активами OSMP: просматривать информацию об активах, искать активы, добавлять активы, редактировать их и удалять, а также экспортировать данные о них в CSV-файл.

С момента добавления актива в OSMP требуется приблизительно 2 минуты, пока решение сможет обогащать этим активом события. Например, если вы добавили актив и в течение двух минут произошло корреляционное событие, в созданном алерте такой актив отображаться не будет.

Категории активов

Вы можете разбить активы по категориям и затем использовать категории в условиях фильтров или правил корреляции. Например, можно создавать алерты более высокого уровня важности для активов из более критичной категории. По умолчанию все активы находятся в категории **Активы без категории**. Устройство можно добавить в несколько категорий.

По умолчанию OSMP категориям активов присвоены следующие уровни критичности: Low, Medium, High, Critical. Вы можете создать пользовательские категории и организовать вложенность.

Категории можно наполнять следующими способами:

- **Вручную**
- **Активно**: динамически, если актив **соответствует заданным условиям**. Например, с момента перехода актива на указанную версию ОС или размещения актива в указанной подсети актив будет перемещен в заданную категорию.

  1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

     Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять, нажав на кнопку **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
OS.	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес;	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
FQDN	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.
ПО	=, like	
КИИ	in	Можно выбрать более одного значения.
Последнее обновление антивирусных баз	>=,<=	
Последнее обновление информации	>=,<=	
Последнее обновление защиты	>=,<=	
Время начала последнего сеанса	>=,<=	
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Состояние постоянной защиты;	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor	=	
Видим в сети	>=,<=	

3. Нажмите на кнопку **Условия проверки**, чтобы убедиться в правильности указанного фильтра. При нажатии на кнопку откроется окно **Активы, найденные по заданным условиям**, содержащее список активов, удовлетворяющих условиям поиска.

- **Реактивно**: при срабатывания корреляционного правила актив будет перемещаться в указанную группу.

В OSMP активы распределены по тенантам и категориям. Активы выстроены в древовидную структуру, где в корне находятся тенанты и от них ветвятся категории активов. Вы можете просмотреть дерево тенантов и категорий в разделе **Активы** → **Все активы**. Если выбрать узел дерева, в правой части окна отображаются активы, относящиеся к соответствующей категории. Активы из подкатегорий выбранной категории отображаются, если вы укажете, что хотите отображать активы рекурсивно. Вы можете выделить флажками тенанты, активы которых хотите просматривать.

Чтобы вызвать контекстное меню категории, наведите указатель мыши на категорию и нажмите на значок с многоточием, который появится справа от названия категории. В контекстном меню доступны следующие действия:

Действия, доступные в контекстном меню категории

Действие	Описание
Показать активы	Просмотреть активы выбранной категории в правой части окна.
Отображать активы рекурсивно	Просмотреть активы из подкатегорий выбранной категории. Если вы хотите выйти из режима рекурсивного просмотра, выберите категорию для просмотра.
О категории	Просмотреть информации о выбранной категории в области деталей **Информация о категории**, которая отображается в правой части окна веб-интерфейса.
Начать категоризацию	Запустить автоматическую привязку активов к выбранной категории. Доступно для категорий с активным способом категоризации.
Добавить подкатегорию	Добавить подкатегорию к выбранной категории.
Изменить категорию	Изменить выбранную категорию.
Удалить категорию	Удалить выбранную категорию. Удалять можно только категории без активов или подкатегорий. В противном случае параметр **Удалить категорию** будет неактивен.
Сделать вкладкой	Отобразить выбранную категорию на отдельной вкладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из вкладок**.

Добавление категории активов

Чтобы добавить категорию активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.

2. Откройте окно создания категории:

   - Нажмите на кнопку **Добавить категорию**.

   - Если вы хотите создать подкатегорию, в контекстном меню родительской категории выберите **Добавить подкатегорию**.

   В правой части окна консоли отобразится область деталей **Добавить категорию**.

3. Добавьте сведения о категории:

- В поле **Название** введите название категории. Название должно содержать от 1 до 128 символов Юникода.

- В поле **Родительская категория** укажите место категории в дереве категорий:

  a. Нажмите на кнопку .

  Откроется окно **Выбор категорий**, в котором отображается дерево категорий. Если вы создаете новую категорию, а не подкатегорию, то в окне может отображаться несколько деревьев категорий активов: по одному для каждого доступного вам тенанта. Выбор тенанта в этом окне невозможно отменить.

  b. Выберите родительскую категорию для создаваемой вами категории.

  c. Нажмите на кнопку **Сохранить**.

  Выбранная категория отобразится в поле **Родительская категория**.

- В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию. Тенанта категории невозможно изменить.

- Назначьте уровень важности категории в раскрывающемся списке **Приоритет**.

- При необходимости в поле **Описание** добавьте примечание: до 256 символов Юникода.

4. В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

- **Вручную** – активы можно привязать к категории только вручную.

- **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

  Активная категория активов

  1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

     Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

  2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

     Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять, нажав на кнопку **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

     Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
OS.	=, like	Оператор like обеспечивает регистронезависимый поиск.

IP-адрес;	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
FQDN	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.
ПО	=, like	
КИИ	in	Можно выбрать более одного значения.
Последнее обновление антивирусных баз	>=,<=	
Последнее обновление информации	>=,<=	
Последнее обновление защиты	>=,<=	
Время начала последнего сеанса	>=,<=	
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Состояние постоянной защиты;	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor	=	
Видим в сети	>=,<=	

3. Нажмите на кнопку **Условия проверки**, чтобы убедиться в правильности указанного фильтра. При нажатии на кнопку откроется окно **Активы, найденные по заданным условиям**, содержащее список активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите на кнопку **Сохранить**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В OSMP можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.

2. В правом верхнем углу таблицы активов нажмите на значок **Параметры** (⚙).

3. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:

   - **Имя**
   - **FQDN**
   - **IP-адрес;**
   - **Категории**
   - **MAC-адрес**
   - **Источник актива**
   - **ОС**
   - **Создан**
   - **Обновлен**
   - **Видим в сети**
   - **Тенант –** когда флажок установлен и столбец отображается в таблице активов, в раскрывающемся списке в столбце **Тенант** доступны следующие параметры фильтрации активов:

     - **Показать только дочерние экземпляры** – будут отображаться только активы дочерних экземпляров в пределах выбранного уровня иерархии тенантов.

     - **Показать только родительские экземпляры** – будут отображаться только активы родительских экземпляров в пределах выбранного уровня иерархии тенантов.

       Эти параметры позволяют фильтровать активы по положению экземпляров в иерархии, к которой они принадлежат, что позволяет сосредоточиться на экземплярах более высокого (родительских) или более низкого уровня (дочерних). Выбранный фильтр сразу применяется к таблице активов.

   - **Категория КИИ**
   - **В архиве –** когда флажок установлен и столбец отображается в таблице активов, в раскрывающемся списке в столбце **В архиве** доступны следующие параметры фильтрации активов:

     - **Да –** отображаются только активы в архивах.

     - **Нет –** отображаются только действующие активы.

   - **Вес**
   - **Группа KSC**

- **Получены данные телеметрии**
- **Статус телеметрии**
- **Статус EDR**
- **Последнее подключение к KSC**
- **Последнее подключение к EDR**
- **Лицензия EDR**
- **Версия EDR-агента**
- **Изоляция EDR**
- **AI-оценка**

Когда вы устанавливаете флажок, таблица активов обновляется и добавляется новый столбец. При снятии флажка столбец исчезает. Таблицу можно сортировать по некоторым столбцам.

4. Если требуется изменить порядок отображения столбцов, зажмите левую клавишу мыши на названии столбца и перетащите его в нужное место таблицы.

Параметры отображения таблицы активов настроены.

Поиск активов

В OSMP есть два режима поиска активов. Переключение между режимами поиска осуществляется с помощью кнопок в верхней левой части окна:

- – простой поиск по параметрам активов **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец**.
- – сложный поиск активов с помощью фильтрации по условиям и группам условий.

Найденные активы можно выделить, установив напротив них флажки, и экспортировать данные о них в виде CSV-файла.

Простой поиск

Чтобы найти актив с помощью простого поиска,

в разделе **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование** введите поисковый запрос в поле **Поиск**.

В таблице отобразятся активы, у которых параметры **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец** соответствуют критериям поиска.

Сложный поиск

Чтобы найти актив с помощью сложного поиска:

1. В разделе **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование** нажмите на значок воронки ( ).

   В верхней части окна отображается блок настройки фильтрации активов.

2. Задайте параметры фильтрации активов и нажмите на кнопку **Поиск**.

   Подробнее о параметрах фильтрации активов см. в таблице ниже.

В таблице отобразятся активы, которые соответствуют критериям поиска.

Сложный поиск активов производится с помощью условий фильтрации, которые можно задать в верхней части окна:

- С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия.
- С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**.
- Условия и группы условий можно перетягивать мышкой.
- Условия, группы и фильтры можно удалить с помощью кнопки ✕.
- Параметры фильтрации можно отобразить в компактно, нажав на кнопку **Свернуть**. В этом случае отображается результирующее поисковое выражение. При нажатии на него условия поиска снова отображаются полностью.
- Параметры фильтрации можно обнулить с помощью кнопки **Очистить**.
- Операторы условий и доступные значения правого операнда зависят от выбранного левого операнда:

Левый операнд	Доступные операторы	Правый операнд
Номер сборки	=, ilike	Произвольное значение.
ОС	=, ilike	Произвольное значение.
IP-адрес	inSubnet, inRange	Произвольное значение или диапазон значений. Условие фильтрации для оператора inSubnet выполнится, если IP-адрес, который содержится в левом операнде входит в подсеть, которая указан в правом операнде. Например, для IP-адреса 10.80.16.206 в правом операнде следует указать подсеть в короткой нотации: `10.80.16.206/25`.
Полное доменное имя	=, ilike	Произвольное значение.
CVE	=, in	Произвольное значение. Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=, <	Число от 0 до 10 (возможные значения уровня критичности уязвимости CVE на активе). Для уязвимостей из Open Single Management Platform неприменимо.

Количество CVE	>, >=, =, <=, <	Число. Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Если в качестве правого операнда указано значение `0` и выбран оператор `=` или `<=`, в результатах поиска будут отображаться активы, у которых отсутствуют уязвимости с CVE.
		Для поиска по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		`CVSS >= 6.5`

ПО	=, ilike	Произвольное значение.
Версия ПО	=, ilike, in	Произвольное значение. Номер версии (сборки) ПО, установленного на активе.
Источник актива	in	• Open Single Management Platform. • KICS/KATA. • Создан вручную.
КИИ	in	• Информационный ресурс не является объектом КИИ. • Объект КИИ без категории значимости. • Объект КИИ третьей категории значимости. • Объект КИИ второй категории значимости. • Объект КИИ первой категории значимости.
ОЗУ (байтов)	=, >, >=, <, <=	Число.
Количество дисков	=, >, >=, <, <=	Число.
Количество сетевых карт	=, >, >=, <, <=	Число.
Свободных байт на диске	=, >, >=, <, <=	Число.
Группа KSC	=, ilike	Произвольное значение. Название группы администрирования Open Single Management Platform, в которую помещен актив.
Последнее обновление антивирусных баз	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе KUMA конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Последнее обновление информации	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе KUMA конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Последнее обновление защиты	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе KUMA конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.

Время начала последнего сеанса	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе KUMA конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Расширенный статус KSC	in	• Устройство с установленным Агентом администрирования подключено к сети, но Агент администрирования неактивен. • Антивирусное приложение установлено, но постоянная защита не работает. • Антивирусное приложение установлено, но не запущено. • Количество обнаруженных вирусов слишком велико. • Антивирусное приложение установлено, но статус постоянной защиты отличается от установленного администратором безопасности. • Антивирусное приложение не установлено. • Полная проверка на вирусы выполнялась слишком давно. • Антивирусные базы обновлялись слишком давно. • Агент администрирования слишком долго был неактивен. • Устаревшая лицензия. • Количество невылеченных объектов слишком велико. • Требуется перезагрузка. • На устройстве установлено одно или несколько несовместимых приложений. • Устройство имеет одну или несколько уязвимостей. • Последний поиск обновлений операционной системы на устройстве выполнялся слишком давно. • Устройство не имеет надлежащего статуса шифрования. • Параметры мобильного устройства не соответствуют требованиям политики безопасности. • Есть необработанные инциденты. • Статус устройства был предложен управляемым приложением. • На устройстве недостаточно места на диске: возникают ошибки синхронизации или на диске недостаточно места.
Статус постоянной защиты	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется). • Выполняется с максимальной защитой. • Выполняется с максимальным быстродействием. • Выполняется с рекомендуемыми параметрами. • Выполняется с пользовательскими параметрами. • Ошибка.
Статус шифрования	=	• На устройстве нет правил шифрования. • Шифрование выполняется. • Шифрование отменено пользователем. • Во время шифрования произошла ошибка. • Все правила шифрования устройства были выполнены. • Шифрование выполняется, на устройстве требуется перезагрузка. • На устройстве есть зашифрованные файлы без указанных правил шифрования.
Статус защиты от спама	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Статус антивирусной защиты почтовых серверов	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Статус защиты данных от утечек	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется.

		• Ошибка. • Не установлено. • Лицензия отсутствует.
Идентификатор расширенного статуса KSC	=	• OK. • Критический. • Требует внимания.
Статус Endpoint Sensor	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Последнее появление в сети	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе KUMA конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Рейтинг AI	=, >, >=, <, <=	Число. Рейтинг активов, присвоенный AI-сервисами.
Статус	=, in	Статусы активов, присвоенные AI-сервисами: • Низкий. • Средний. • Высокий. • Критический.
Настраиваемое поле актива	=, ilike	Произвольное значение. Поиск по настраиваемым полям активов.

Использование временных значений

Некоторые условия, например, **Последнее обновление антивирусных баз** или **Время начала последней сессии**, используют дату и время в качестве значения операнда. Для этих условий вы можете использовать точные дату и время или относительный период.

Чтобы указать значение даты и времени:

1. Выберите необходимый операнд, оператор и нажмите на поле даты.

2. Выполните одно из следующих действий:

   - В календаре выберите точную дату.

     По умолчанию к выбранной дате будет автоматически добавлено текущее время с точностью до миллисекунд. При изменении даты в календаре указанное время не меняется. Дата и время отображаются в соответствии с часовым поясом браузера. При необходимости вы можете изменить дату и время в поле вручную.

   - В списке **Относительный период** выберите относительный период.

     Период рассчитывается относительно текущего времени поиска и учитывает актуальную на этот момент информацию об активах. Например, для условия **Последнее обновление антивирусных баз** вы можете выбрать значение **1 час** и оператор **>=**, чтобы найти активы, для которых антивирусные базы не обновлялись более 1 часа.

   - В поле даты и времени введите значение вручную.

Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или относительный период в виде формулы. При необходимости вы также можете комбинировать эти способы.

Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически.

В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени и язык параметризации интервалов: символы **+**, **-**, **/** (округление до ближайшего), а также единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда).

Например, для условия **Последнее обновление информации** вы можете указать значение **now-2d** с оператором **>=** и значение **now-1d** с оператором **>=**, чтобы найти активы, информация о которых обновилась за сутки до запуска поиска; или указать значение **now/w** с оператором **<=**, чтобы найти активы, информация о которых обновилась с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

Время в KUMA хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период **Сегодня**, в категорию будут попадать активы за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите при категоризации учитывать ваш часовой пояс, вам нужно вручную добавить сдвиг по времени в поле даты и времени, прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите при категоризации учитывать период **Вчера**, вам нужно изменить значение на **now-1d/d-3h**. Если же вы хотите при категоризации учитывать период **Сегодня** – на **now/d-3h**.

Экспорт данных об активах

Данные об активах, отображаемых в таблице активов, можно экспортировать в виде CSV-файла.

Чтобы экспортировать данные об активах:

1. Настройте таблицу активов.

   В файл записываются только данные, указанные в таблице. Порядок отображения столбцов таблицы активов повторяется в экспортированном файле.

2. Найдите нужные активы и выберите их, установив рядом с ними флажки.

   При необходимости вы можете выбрать сразу все активы в таблице, установив флажок в левой части заголовка таблицы активов.

3. Нажмите на кнопку **Экспортировать в CSV**.

Данные об активах будут записаны в файл assets_<дата экспорта>_<время экспорта>.csv. Файл будет скачан в соответствии с параметрами вашего браузера.

Просмотр информации об активе

Чтобы просмотреть информацию об активе, откройте окно информации об активе одним из следующих способов:

- В главном меню перейдите в раздел **Управление активами**, выберите категорию с нужными активами и выберите актив.
- В главном меню выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
- В главном меню выберите раздел **События** → выполните поиск и фильтрацию событий → выберите требуемое событие → нажмите на ссылку в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.

В окне информации об активе может отображаться следующая информация:

- **Название, ID** – имя актива, идентификатор.

  Активы, импортированные в OSMP, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить имена активов в веб-интерфейсе OSMP.
- **Тенант** – название тенанта, которому принадлежит актив.
- **Архивный** – статус архивации актива. Доступные значения: Да, Нет.
- **Группа KSC** – группа Серверов KSC, к которой относится актив.
- **Источник актива** – источник информации об активе. Источников может быть несколько: сведения можно добавить в веб-интерфейсе OSMP или с помощью API, а также импортировать из Open Single Management Platform и KICS/KATA.

  Добавляя в OSMP сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.
- **Создан** – дата и время добавления актива в OSMP.
- **Последнее обновление** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если есть).

  > Если в OSMP есть несколько активов с одинаковыми IP-адресами, актив, добавленный позже, возвращается во всех случаях поиска активов по IP-адресу. Если в сети вашей организации допустимо наличие активов с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации активов. Это может оказаться важным при корреляции.
- **Полное доменное имя** – полностью определенное имя домена актива, если указано.
- **MAC-адрес** – MAC-адрес актива (если есть).
- **Операционная система** – операционная система актива.

- **AI-оценка** – число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля **AI-статус**: **Low**, **Medium**, **High**, **Critical**. Значение рейтинга может быть от 0 до 1.

- **Статус изоляции** – статус сетевой изоляции актива. Вы можете просмотреть и изменить состояние сетевой изоляции устройства, перейдя по ссылке **Параметры** рядом со статусом. Поле отображается, если приложение Kaspersky Endpoint Security со встроенным агентом установлено на активе (устройстве).

- **Категория КИИ** – сведения о том, является ли актив объектом критической информационной инфраструктуры (КИИ).

- **Связанные алерты** – алерты, с которыми связан актив (если есть).

  Для просмотра списка алертов, с которыми связан актив, можно перейти по ссылке **Найти в алертах**. Откроется вкладка **Алерты** с поисковым выражением, позволяющим отфильтровать все активы с соответствующим идентификатором.

- **Информация о программном обеспечении** и **Информация об оборудовании** – если указаны параметры программного обеспечения и оборудования актива, они отображаются в этом разделе.

- Сведения об уязвимостях актива:

  - **Уязвимости Kaspersky Security Center** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Open Single Management Platform.

    Вы можете узнать больше об уязвимости, нажав на значок , открывающий портал Kaspersky Threats. Вы также можете обновить список уязвимостей, нажав на ссылку **Обновить** и запросив обновленную информацию из Open Single Management Platform.

  - **Уязвимости KICS/KATA** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS/KATA.

- Сведения об источниках актива:

  - **Последнее появление в сети** – время последнего получения сведений об активе из Open Single Management Platform. Эта информация доступна для активов, импортированных из Open Single Management Platform.

  - **Идентификатор хоста** – идентификатор *агента администрирования* Open Single Management Platform, от которого получены сведения об активе. Эта информация доступна для активов, импортированных из Open Single Management Platform. С помощью этого идентификатора определяется уникальность актива в Open Single Management Platform.

  - **IP-адрес сервера KICS/KATA** и **Идентификатор коннектора KICS/KATA** – данные об экземпляре KICS/KATA, из которого был импортирован актив.

- **Настраиваемые поля** – данные, записанные в настраиваемые поля активов.

- Дополнительные сведения о параметрах защиты актива с установленного приложения Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux:
  - **Идентификатор расширенного статуса KSC** – статус актива. Может иметь следующие значения:
    - OK.
    - Критическое.
    - Предупреждение.
  - **Расширенный статус KSC** – информация о состоянии актива. Например, **Антивирусные базы обновлялись слишком давно**.
  - **Статус постоянной защиты** – статус программ "Лаборатории Касперского", установленных на активе. Например, **Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется)**.
  - **Статус шифрования** – информация о шифровании актива. Например, **На хосте нет правил шифрования**.
  - **Статус защиты от спама** – состояние защиты от спама. Например, **Запущена**.
  - **Статус антивирусной защиты почтовых серверов** – состояние антивирусной защиты почтовых серверов. Например, **Запущена**.
  - **Статус защиты данных от утечек** – состояние защиты данных от утечек. Например, **Запущена**.
  - **Статус Endpoint Sensor** – состояние защиты данных от утечек. Например, **Запущена**.
  - **Последнее обновление антивирусных баз** – версия загруженных антивирусных баз.
  - **Последнее обновление защиты** – время последнего обновления антивирусных баз.
  - **Время начала последней сессии** – время последнего запуска системы.
  - **Последнее обновление информации** – время последнего появления актива в сети. Для поиска время приводится в UTC, и затем в интерфейсе конвертируется в соответствии с локальным часовым поясом, установленным в браузере.

  Эти сведения отображаются, если актив был импортирован из Open Single Management Platform.
- **Категории** – категории, к которым относится актив (если есть).

По кнопке **Переместить в группу KSC** вы можете переместить просматриваемый актив между группами администрирования Open Single Management Platform. Вы также можете нажать на раскрывающийся список **Запустить задачу**, чтобы запустить выполнение доступных на активе задач:

- По кнопке **Реагирование KSC** вы можете запустить на активе выполнение задачи Open Single Management Platform.
- По кнопке **Реагирование KEDR** вы можете запустить на активе выполнение задачи в Kaspersky Endpoint Detection and Response.
- По кнопке **Обновить KSC актив** вы можете запустить на активе задачу обновления информации о нем из Open Single Management Platform.

Задачи доступны при интеграции с Open Single Management Platform и при интеграции с Kaspersky Endpoint Detection and Response.

Добавление активов

Вы можете добавлять информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в Консоли OSMP или с помощью API.

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center, KICS for Networks и MaxPatrol VM.

При добавлении активы, уже существующие в OSMP, могут объединяться с добавляемыми активами.

Алгоритм объединения активов:

1. Проверка на уникальность активов в Kaspersky Security Center или KICS for Networks активов:

   - Уникальность актива импортированного из Kaspersky Security Center, проверяется по параметру **Идентификатор устройства**, в котором указан идентификатор *агента администрирования* Kaspersky Security Center. Если идентификаторы у двух активов различаются, активы считаются разными, объединения данных не происходит.

   - Уникальность актива импортированного из KICS for Networks, определяется по комбинации параметров **IP-адрес**, **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks**. Если любой из параметров у двух активов различается, активы считаются разными, объединения данных не происходит.

   Если активы совпадают, алгоритм выполняется далее.

2. Проверка на совпадение значений в полях **IP**, **MAC**, **FQDN**.

   Если хотя бы два из указанных полей совпадают, активы объединяются при условии, что другие поля не заполнены.

Возможные варианты совпадений:

- FQDN и IP-адрес активов. Поле **MAC** не заполнено.

  Проверка производится по всему массиву значений IP-адресов. Если IP-адрес актива входит в состав FQDN, значения считаются совпавшими.

- FQDN и MAC-адрес активов. Поле **IP** не заполнено.

  Проверка производится по всему массиву значений MAC-адресов. При полном совпадении хотя бы одного значения массива с FQDN значения считаются совпавшими.

- IP-адрес и MAC-адрес активов. Поле **FQDN** не заполнено.

  Проверка производится по всему массиву значений IP- и MAC-адресов. При полном совпадении хотя бы одного значения в массивах значения считаются совпавшими.

3. Проверка на совпадение хотя бы одного из полей **IP**, **MAC**, **FQDN** при условии, что два других поля не заполнены для одного или обоих активов.

   Активы объединяются, если значения в поле совпадают. Например, если для актива KUMA указаны FQDN и IP-адрес, а для импортируемого актива только IP-адрес с тем же значением, поля считаются совпавшими. В этом случае активы объединяются.

   Для каждого поля проверка производится отдельно и завершается при первом совпадении.

Вы можете посмотреть примеры сравнения полей активов здесь.

Информация об активах может формироваться из разных источников. Если добавляемый актив и актив OSMP содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в OSMP получил полное доменное имя и информацию о программном обеспечении. При импорте актива из Kaspersky Security Center с аналогичным полным доменным именем эти данные будут перезаписаны при условии, что они указаны для добавляемого актива. Все поля, в которых могут обновляться данные, приведены в таблице Обновляемые данные.

Обновляемые данные

Название поля	Принцип обновления
Имя	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS for Networks.
Владелец	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
IP-адрес;	Данные объединяются. Если в массиве адресов есть одинаковые адреса, копия дублирующегося адреса удаляется.
FQDN	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.

Название поля	Принцип обновления
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
Уязвимости	Данные активов KUMA дополняются информацией из добавляемых активов. В информации об активе данные группируются по названию источника. Устранение уязвимостей для каждого источника осуществляется отдельно.
Информация о программном обеспечении	Данные из KICS for Networks записываются всегда (при наличии). Для других источников выбирается первое значение согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
Информация об оборудовании	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано через API.

Обновленные данные отображаются в информации об активе. Вы можете просмотреть информацию об активе в Консоли OSMP.

При добавлении новых активов эти данные могут быть перезаписаны. Если данные, из которых сформирована информация об активе, не обновляются из источников более 30 дней, актив удаляется. При следующем добавлении актива из тех же источников создается новый актив.

При изменении в Консоли OSMP активов, информация о которых получена из Kaspersky Security Center или KICS for Networks, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в Консоли OSMP этих активов вы можете изменить следующие данные актива:

- Название.
- Название тенанта, которому принадлежит актив.
- IP-адрес.
- Полное доменное имя.
- MAC-адрес.
- Владелец.
- Категория.
- Операционная система.
- Информация об оборудовании.

Редактирование данных об активах через REST API недоступно. При импорте из REST API происходит обновление данных по правилам слияния информации об активах, приведенным выше.

Добавление информации об активах в OSMP

Чтобы добавить актив в OSMP:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование** и нажмите **Добавить**.

   В правой части окна откроется область деталей **Добавить актив**.

2. Введите параметры актива:

   - **Имя актива** (обязательно).
   - **Тенант** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN, нажав на кнопку **Добавить FQDN**.
   - **MAC-адрес.**
   - **Владелец.**

3. При необходимости заполните парамерты на следующих вкладках:

   - **Дополнительные** — сведения о владельце, категории, операционной системе актива.
   - **Оборудование** — сведения об оборудовании актива.

4. Нажмите на кнопку **Добавить**.

   Актив создан и отображается в таблице активов в назначенной ему категории или в категории **Активы без категории**.

Импорт информации об активах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой этого приложения. Вы можете импортировать информацию об активах, защищаемых Kaspersky Security Center, в KUMA. Для этого вам требуется предварительно настроить интеграцию между приложениями.

KUMA импортирует следующие данные об устройстве, полученные от Агентов администрирования Kaspersky Security Center:

- основную информацию об активе – имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании, состоянии защиты, версии антивирусных баз;
- информацию об атрибутах актива – об уязвимостях, о программном обеспечении, включая операционную систему, о владельцах.

Чтобы импортировать информацию об активах Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.

2. Нажмите **Импортировать** и выберите одно из следующих действий:

   - Чтобы импортировать информацию об основных атрибутах активов, нажмите **Импортировать активы KSC**.

     Откроется окно **Импорт активов KSC**.

   - Чтобы импортировать информацию о других атрибутах активов, нажмите **Импортировать атрибуты активов KSC**.

     Откроется окно **Импортировать атрибуты активов KSC**.

3. В раскрывающемся списке выберите тенант, для которого вы хотите выполнить импорт.

   В этом случае приложение загружает информацию обо всех активах всех Серверов администрирования Kaspersky Security Center, для которых настроено подключение к выбранному тенанту.

   Если вы хотите импортировать информацию обо всех активах всех Серверов администрирования Kaspersky Security Center для всех тенантов, выберите **Все**.

4. Нажмите на кнопку **Импортировать**.

Информация об активах будет импортирована.

Также в окне свойств тенанта вы можете настроить периодический импорт информации об активах или запустить импорт вручную.

Импорт информации об активах из KICS for Networks

Вы можете импортировать информацию об активах, защищаемых KICS for Networks, в KUMA. Для этого вам требуется предварительно настроить интеграцию между приложениями.

После создания интеграции с KICS for Networks задачи на получение данных об активах KICS for Networks создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную.

Чтобы настроить задачу на обновление данных об активах KICS for Networks для тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Выберите тенант, для которого вы хотите импортировать активы KICS/KATA.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Параметры активов**.

4. Убедитесь, что на вкладке **Импорт KICS/KATA** включен переключатель **Состояние**.

5. Настройте импорт данных актива:

   - Чтобы настроить периодический импорт данных, в поле **Интервал импорта (в часах)** укажите интервал, через который OSMP будет обновлять данные об активах KICS/KATA.

   - Чтобы запустить импорт вручную, нажмите на кнопку **Импорт**.

В Консоли OSMP в разделе Диспетчер задач будет добавлена **задача** на получение данных об учетных записях выбранного тенанта.

Примеры сравнения полей активов при импорте

Каждый импортируемый актив сравнивается с активом OSMP.

Проверка на совпадение значений в полях IP, MAC, FQDN по двум полям

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Есть	Есть	Не заполнено
Импортируемый актив 1	Есть, совпадает	Есть, совпадает	Есть
Импортируемый актив 2	Есть, совпадает	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть, совпадает	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Есть, совпадает	Есть
Импортируемый актив 5	Есть, совпадает	Не заполнено	Не заполнено
Импортируемый актив 6	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и IP, по полю MAC нет противоречия. Активы объединены.

- Импортируемый актив 2 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и IP. Активы объединены.

- Импортируемый актив 3 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и MAC, по полю IP нет противоречия. Активы объединены.

- Импортируемый актив 4 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.

- Импортируемый актив 5 и актив OSMP: для обоих активов заполнено и совпадает поле FQDN, по полям IP и MAC нет противоречия. Активы объединены.

- Импортируемый актив 6 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.

Проверка на совпадение значений в полях IP, MAC, FQDN по одному полю

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив OSMP	Не заполнено	Есть	Не заполнено
Импортируемый актив 1	Есть	Есть, совпадает	Есть
Импортируемый актив 2	Есть	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 2 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 3 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.
- Импортируемый актив 4 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.

Назначение активу категории

Назначение категории одному активу в свойствах актива

Этот способ не подходит для назначения категории активам KSC и KICS. Следуйте инструкции по назначению категории одному или нескольким активам.

Чтобы назначить категорию одному активу:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.
2. Нажмите на кнопку **Показать навигацию** и выберите тенант и категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив и в открывшемся меню выберите **Подробнее**.
4. В открывшемся окне нажмите на кнопку **Изменить**.

5. На вкладке **Дополнительные** в поле **Категории** выберите категорию.

> Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку ✕.

6. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Назначение категории одному или нескольким активам

Чтобы назначить категорию одному или нескольким активам:

1. В главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.
2. Нажмите на кнопку **Показать навигацию** и выберите тенант и категорию с требуемыми активами.

   Отобразится таблица активов.
3. Установите флажки рядом с активами, для которых вы хотите изменить категорию.
4. Нажмите на кнопку **Привязать к категории**.
5. В открывшемся окне выберите категорию.
6. Нажмите на кнопку **Привязать**.

Категория будет назначена.

> Не назначайте активам категорию `Categorized assets`.

Привязка группы активов к категории

Чтобы привязать группу активов к категории:

1. В разделе **Управление активами** в заголовке таблицы со списком активов установите флажок.
2. Выделите все активы, видимые на странице или все активы, согласно условию выбора.

   Кнопка **Привязать к категории** становится активной и открывает доступные категории.
3. Нажмите на кнопку **Привязать к категории** и выберите одну или несколько категорий для привязки.
4. Нажмите **OK**.

   Активы привязываются к выбранным категориям или папке.

Отвязка группы активов от категории

Чтобы отвязать группу активов от категории:

1. Выберите одну категорию (тенант) в навигационной панели.

   Отображается список активов категории.

   В свойства папки добавится кнопка **Очистить категорию**.

2. В контекстном меню категории выберите **Очистить категорию**.

   Появляется диалоговое окно с запросом подтверждения и числом отвязываемых активов.

   Эта опция позволяет отвязывать все активы в выбранной категории, не только видимые на странице. Активы в дочерних категориях не отвязываются.

3. В диалоговом окне нажмите **OK**.

   Все выбранные активы будут отвязаны от выбранной категории.

Изменение параметров активов

В OSMP можно изменять параметры активов. У добавленных вручную активов можно изменять все параметры. У активов, импортированных из Kaspersky Security Center, можно изменить только название актива и его категорию.

Чтобы изменить параметры актива:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.

2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.

3. Выберите актив и нажмите **Сведения**.

4. В открывшемся окне нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

5. Внесите необходимые изменения в доступные поля:

   - **Название актива** (обязательно). Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS for Networks.

   - **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN через запятую.

   - **MAC-адрес.**

   - **Владелец.**

- **Информация о программном обеспечении**:
  - **Название ОС**
  - **Сборка ОС**
- **Информация об оборудовании**:

  Параметры оборудования

  В раздел **Информация об оборудовании** можно добавить сведения об оборудовании актива:

  Доступные поля для описания CPU актива:

  - **Название процессора**
  - **Частота процессора**
  - **Количество ядер процессора**

    Активу можно добавить процессоры с помощью кнопки **Добавить процессор**.

  Доступные поля для описания диска актива:

  - **Свободных байт на диске**
  - **Объем диска**

    Активу можно добавить диски с помощью кнопки **Добавить диск**.

  Доступные поля для описания RAM актива:

  - **Частота оперативной памяти**
  - **Общий объем ОЗУ**

  Доступные поля для описания сетевой карты актива:

  - **Название сетевой карты**
  - **Производитель сетевой карты**
  - **Версия драйвера сетевой карты**

    Активу можно добавить сетевые карты с помощью кнопки **Добавить сетевую карту**.
- Настраиваемые поля.
- Категория КИИ.

6. На вкладке **Дополнительные** в поле **Категории** выберите категорию.

> Также можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

Не назначайте активам категорию `Categorized assets`.

7. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Архивирование активов

В OSMP функция архивирования доступна для следующих типов активов:

- Для активов, импортированных из Kaspersky Security Center и KICS.

  Если после десяти попыток импорта OSMP не смогла получить информацию об активе, актив автоматически переводится в состояние архивного и хранится в базе данных в течение срока, который вы можете задать в параметре **Срок хранения архивных активов**. Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно Архивный актив станет активным, если OSMP получит информацию об активе от источника до истечения срока хранения архивных активов.

- Для объединенных активов.

  При импорте OSMP выполняет проверку на уникальность среди активов, импортированных из Kaspersky Security Center и KICS, и активов, добавленных вручную. Если поля импортированного актива и добавленного вручную актива совпадают, активы объединяются в один актив, который считается импортированным и может стать архивным.

- Активы, добавленные вручную в консоли или с помощью API, архивируются и хранятся в базе данных в течение периода, указанного в параметре **Срок хранения архивных активов (в днях)**. Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно Вы можете использовать параметр **Разархивировать активы**, если хотите сделать актив действующим до истечения срока хранения архивных активов.

Актив становится архивным при следующих условиях:

- Вы используете параметр **Архивировать активы** для активов, созданных вручную в консоли или с помощью API.

- Приложение OSMP не получило информацию об активе от Kaspersky Security Center или KICS for Networks после десяти попыток импорта.

- Отключена интеграция с Kaspersky Security Center.

  Если вы отключили интеграцию с Kaspersky Security Center, в течение 30 дней актив будет считаться активным. По истечении 30 дней актив автоматически переводится в состояние архивного и хранится в базе данных в течение времени, указанного в параметре **Срок хранения архивных активов (в днях)**.

Обновление актива не происходит в следующих случаях:

- Данные об активе Kaspersky Security Center не обновлялись больше срока хранения архивных активов.

- Данные об активе отсутствуют в Kaspersky Security Center или KICS for Networks.

- Соединение с Сервером администрирования Kaspersky Security Center отсутствует больше 30 дней.

Чтобы изменить статус архива для актива или группы активов, созданных вручную:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Анализ и реагирование**.

   Откроется таблица активов.

2. В таблице активов установите флажки рядом с активами, созданными вручную, для которых вы хотите изменить статус архивирования.

3. На панели инструментов в верхней части таблицы ресурсов нажмите на одну из следующих кнопок:

   - **Архивирование активов**, чтобы поместить выбранные активы в архив.

   - **Разархивировать активы**, чтобы восстановить выбранные архивные активы.

   Архивный статус актива изменен. Вы можете отфильтровать активы по их архивному статусу в таблице активов в раскрывающемся списке столбца **Архивированные**, выбрав один из вариантов: **Да**, чтобы отображать только архивные активы, или **Нет**, чтобы отображать только действующие активы.

Чтобы настроить срок хранения архивных активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Параметры активов**.

4. На вкладке **Общая** введите новое значение в поле **Срок хранения архивных активов (в днях)**.

   Значение по умолчанию – 30 дней. Введите значение 0, чтобы хранить архивные активы бессрочно.

5. Нажмите на кнопку **Сохранить**.

   Срок хранения архивных активов будет настроен.

Информация об архивном активе остается доступной для просмотра в карточке алертов и инцидентов.

Чтобы просмотреть карточку архивного актива:

1. В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**.

   Отобразится список алертов или инцидентов.

2. Откройте карточку алерта или инцидента, связанного с архивным активом.

   Вам будет доступен просмотр информации в карточке архивного актива.

Удаление активов

Вы можете удалять активы на вкладке **Администрирование и защита**. На вкладке **Обнаружение и реагирование** OSMP удаляет только архивные активы только автоматически. Удалить активы вручную невозможно. OSMP удалит архивный актив, если информация об активе не обновлялась больше срока хранения архивных активов.

Удаление категории активов

Удаление категории выполняется в два этапа: перемещение в архив и безвозвратное удаление. Архивирование позволяет проверить, ссылаются ли на категорию какие-либо ресурсы, прежде чем она будет окончательно удалена из системы.

Если категория архивируется в родительском экземпляре OSMP, соответствующая категория во всех дочерних экземплярах OSMP также архивируется. Затем система проверяет, ссылаются ли все еще какие-либо ресурсы на заархивированную категорию. Если не осталось ссылок, категория будет удалена безвозвратно.

Чтобы удалить категорию активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.

2. В дереве категорий нажмите на значок (⋮) рядом с категорией, которую вы хотите удалить.

3. В контекстном меню нажмите **Архив**.

4. В диалоговом окне **Удалить категорию?** нажмите на кнопку **OK** для подтверждения.

Если ресурсы все еще привязаны к категории, категория остается в архиве до тех пор, пока не будут удалены все связи.

Заархивированные категории не отображаются в списке категорий, но могут оставаться доступными в фильтрах, которые ссылаются на категорию. Свойства категории остаются доступными для просмотра, а связи ресурсов можно удалить. Изменение параметров категории невозможно, кроме названия категории.

Дополнительные ограничения применяются к категориям, содержащим дочерние категории:

- Родительская категория не может быть перемещена в архив или удалена, если в ней есть хотя бы одна дочерняя категория, не перемещенная в архив.

- Перед удалением родительской категории все дочерние категории должны быть заархивированы или удалены без возможности восстановления.

- После того как все дочерние категории перемещены в архив, родительская категория следует стандартному процессу перемещения в архив и удаления.

Категория удаляется безвозвратно только если все ссылки на категорию удалены и все ограничения иерархии выполнены.

Массовое удаление активов

В веб-интерфейсе OSMP вы можете осуществить множественный выбор активов с помощью фильтра и удалить все выбранные активы.

Для удаления активов у вас должны быть права на удаление активов.

Массовое удаление активов

Чтобы удалить все выбранные активы:

1. В главном окне приложения перейдите в раздел **Управление активами** и выберите категорию с требуемыми активами.

   Отобразится таблица со списком активов.

2. В шапке таблицы со списком активов установите флажок.

   Вам будет предложено два варианта удаления: все активы или все активы, видимые на странице.

3. Нажмите на **Выбрать все на странице** или **Выбрать все**.

   Кнопка **Удалить** станет активной.

4. Нажмите на кнопку **Удалить**.

   Появится окно с запросом подтверждения удаления и с информацией о том, что удаленные активы не будут доступны в алертах, инцидентах и виджетах.

   Внизу страницы отобразится количество выбранных для удаления активов.

5. Нажмите **OK**.

   Если вы нажали на **Выбрать все**, то перед подтверждением удаления нужно ввести запрашиваемую сгенерированную строку в текстовое поле окна.

Все выбранные активы будут удалены.

Удаление папок с активами

Для удаления папки вы можете или отвязать (при этом активы будут отвязаны, но не удалены) все активы от папки и затем удалить саму папку, или удалить все активы (активы будут удалены из программы), а затем удалить папку.

Обновление приложений сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять приложения сторонних производителей, в том числе приложения Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих приложений.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Приложение – Kaspersky Security Center.
- Тип задачи – *Установка требуемых обновлений и закрытие уязвимостей*.
- Устройства, которым будет назначена задача – вам требуется назначить задачу корневой группе администрирования.

- Правила для установки обновлений:
  - Устанавливать только утвержденные обновления.
  - Закрывать уязвимости с уровнем критичности равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.
- Запуск по расписанию – расписание, в соответствии с которым выполняется задача.

О способах создания задачи см. подробнее в *справке Kaspersky Security Center*.

> Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Далее вам требуется установить обновления для приложений сторонних производителей и закрыть уязвимости на активах в OSMP.

Чтобы установить обновления и закрыть уязвимости приложений сторонних производителей на активе в OSMP:

1. Откройте окно информации об активе одним из следующих способов:
   - В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**, выберите категорию с соответствующими активами, затем выберите актив и нажмите **Подробнее**.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**. Выполните поиск и фильтрацию событий. Затем выберите требуемое событие и перейдите по ссылке в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.
2. В окне информации об активе раскройте список **Уязвимости Kaspersky Security Center**.
3. Установите флажки рядом с приложениями, которые вы хотите обновить.
4. Нажмите на ссылку **Загрузить обновления**.
5. В открывшемся окне установите флажок рядом с идентификатором уязвимости, которую вы хотите закрыть.
6. Если в столбце **Лицензионное соглашение принято** для выбранного идентификатора отображается **Нет**, нажмите на кнопку **Принять обновления**.
7. Перейдите по ссылке в столбце **URL Лицензионного соглашения** и ознакомьтесь с текстом Лицензионного соглашения.
8. Если вы с ним согласны, нажмите **Принять Лицензионные соглашения**.

   Напротив идентификатора уязвимости, для которого было принято Лицензионное соглашение, в столбце **Лицензионные соглашения приняты** отобразится **Да**.

9. Повторите шаги 7–10 для каждого требуемого идентификатора уязвимости.

10. Нажмите на кнопку **OK**.

Обновления будут загружены и установлены на активы, того сервера Администрирования, где была запущена задача, а также на активы всех подчиненные серверы Администрирования.

> Условия Лицензионного соглашения для обновления и закрытия уязвимостей требуется принять на каждом подчиненном сервере Администрирования отдельно.

Обновления устанавливаются на активы, на которых была обнаружена уязвимость.

Вы можете обновить список уязвимостей для актива в окне информации об активе, нажав на ссылку **Обновить**.

Перемещение активов в выбранную группу администрирования

Вы можете перемещать активы в выбранную группу администрирования Kaspersky Security Center. В этом случае на активы будут распространятся групповые политики и задачи. Подробнее о политиках и задачах Kaspersky Security Center см. *справку Kaspersky Security Center*.

Группы администрирования добавляются в OSMP при загрузке иерархии во время импорта активов из Kaspersky Security Center. Предварительно вам требуется настроить интеграцию OSMP с Kaspersky Security Center.

Чтобы переместить один актив в выбранную группу администрирования:

1. Откройте окно информации об активе одним из следующих способов:

   - В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**, выберите категорию с соответствующими активами, затем выберите актив и нажмите **Подробнее**.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Алерты**, перейдите по ссылке с соответствующим алертом, затем в разделе **Активы** выберите актив и нажмите на кнопку **Просмотреть свойства**.

2. В окне информации об активе нажмите **Реагирование** → **Переместить в группу**.

3. В открывшемся окне выберите группу.

   > Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.

4. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

Чтобы переместить несколько активов в выбранную группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.
2. Выберите категорию с требуемыми активами.
3. Установите флажки рядом с активами, которые хотите переместить в группу.
4. Нажмите **Реагирование** → **Переместить в группу**.

   Кнопка активна, если все выбранные активы принадлежат одному серверу Администрирования.

5. В открывшемся окне выберите группу.
6. Нажмите на кнопку **Сохранить**.

Выбранные активы будут перемещены.

Вы можете посмотреть, к какой группе принадлежит актив, в информации об активе.

Сведения об активах Kaspersky Security Center обновляются в OSMP в момент импорта информации об активах из Kaspersky Security Center. Это означает, что может возникнуть ситуация, когда в Kaspersky Security Center активы были перемещены между группами администрирования, однако в OSMP эти сведения еще не отображаются. При попытке переместить такой актив в группу администрирования, в которой он уже находится, OSMP возвращает ошибку **Не удалось переместить активы в другую группу KSC**.

Аудит активов

В OSMP можно настроить создание событий аудита активов при следующих условиях:

- Актив добавлен в OSMP. Отслеживается создание актива вручную, а также создание при импорте через REST API, импорте из Kaspersky Security Center или KICS for Networks.
- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:
  - Имя
  - IP-адрес;
  - MAC-адрес.
  - FQDN
  - Операционная система

  Изменения полей может происходить при обновлении актива во время импорта.

- Актив удален из OSMP. Отслеживается удаление активов вручную, а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS for Networks, данные о которых перестали поступать.

- Сведения об уязвимости добавлены в актив. Отслеживается появление у активов новых данных об уязвимостях. Сведения об уязвимостях могут быть добавлены в актив, например, при импорте активов из Kaspersky Security Center или KICS for Networks.

- Уязвимость актива закрыта. Отслеживается удаление из актива сведений об уязвимости. Уязвимость считается закрытой, если данные о ней перестают поступать из всех источников, из которых ранее были получены сведения о ее появлении.

- Актив добавлен в категорию. Отслеживается присвоении активу категории активов.

- Актив удален из категории. Отслеживается удаление актива из категории активов.

По умолчанию, если аудит активов включен, при описанных выше условиях OSMP создает не только события аудита (`Type = 4`), но и базовые события (`Type = 1`).

События аудита активов можно отправлять, например, на хранение или в корреляторы.

Настройка аудита активов

Чтобы настроить аудит активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Выберите тенант, для которого вы хотите настроить аудит активов.

   Откроется окно свойств тенанта.

   Если вы хотите настроить аудит активов для нового тенанта, сначала создайте его.

3. На вкладке **Параметры** нажмите на **Аудит активов**.

4. Выберите для каждого условия создания событий аудита активов, куда будут отправляться создаваемые события:

   a. В блоке параметров нужного типа событий аудита активов в раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, куда следует отправлять создаваемые события:

      - Выберите **Хранилище**, если хотите, чтобы события отправлялись в хранилище.

      - Выберите **Коррелятор**, если хотите, чтобы события отправлялись в коррелятор.

      - Выберите **Другое**, если хотите выбрать иную точку назначения.

      > К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Откроется окно **Добавить точку назначения**, где вам требуется параметры пересылки событий.

b. В раскрывающемся списке **Точка назначения** выберите существующую точку назначения или выберите пункт **Создать**, если хотите создать точку назначения.

   При создании новой точки назначения заполните параметры, как указано в описании точки назначения.

c. Нажмите на кнопку **Сохранить**.

Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения.

5. Нажмите на кнопку **Сохранить**.

Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Нажмите на кнопку **Сохранить**.

Хранение и поиск событий аудита активов

События аудита активов считаются базовыми и не заменяют собой событий аудита. События аудита активов можно искать по следующим параметрам:

Поле события	Значение
DeviceVendor	`"Лаборатория Касперского".`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Включение и выключение аудита активов

Вы можете включить или выключить аудит активов для тенанта.

Чтобы включить или выключить аудит активов для тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите включить или выключить аудит активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Аудит активов**.
4. Включите или выключите переключатель **Сбор событий аудита**.
5. Нажмите на кнопку **Сохранить**.

По умолчанию при включенном аудите активов при возникновении условия аудита одновременно создаются два типа событий: базовое событие и событие аудита.

Вы можете отключить создание базовых событий одновременно с событиями аудита.

Чтобы включить или выключить для отдельного условия создание базовых событий:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите включить или выключить условие для генерации событий аудита активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Аудит активов**.
4. Нажмите имя действия с условием, чтобы включить или выключить создание соответствующих базовых событий.
5. Нажмите на кнопку **Сохранить**.

Если условие выключено, создаются только события аудита, базовые события создаваться не будут.

Настраиваемые поля активов

В дополнение к существующим полям модели данных актива можно создать настраиваемые поля активов. Данные из настраиваемых полей активов отображаются при просмотре информации об активе. Данные в настраиваемые поля можно записывать вручную или через API.

Вы можете создать или изменить настраиваемые поля в OSMP в разделе **Активы** в таблице **Настраиваемые поля**. Таблица имеет следующие столбцы:

- **Название** – название настраиваемого поля, которое отображается при просмотре информации об активе.
- **Значение по умолчанию** – значение, которое записывается в настраиваемое поле при добавлении актива в KUMA.
- **Маска** – регулярное выражение, которое должно совпадать со значением, записываемым в поле.

Чтобы создать настраиваемое поле активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Параметры активов**.
4. На вкладке **Общая** в поле **Пользовательские поля** нажмите на кнопку **Добавить**.

   В таблице **Пользовательские поля** добавится пустая строка. Вы можете добавить сразу несколько строк с параметрами настраиваемого поля.

5. Заполните столбцы с параметрами настраиваемого поля:

   - **Название** (обязательно) – от 1 до 128 символов Юникода.
   - **Значение по умолчанию** – от 1 до 1024 символов Юникода.
   - **Маска** – от 1 до 1024 символов Юникода.

6. Нажмите на кнопку **Сохранить**.

   К модели данных активов добавлено настраиваемое поле.

Чтобы удалить или изменить настраиваемое поле активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Параметры активов**.
4. На вкладке **Общие** внесите необходимые изменения в таблицу **Настраиваемые поля**:

   - Чтобы удалить настраиваемое поле, установите флажок рядом с нужным полем и нажмите на кнопку **Удалить**. При удалении поля также удаляются записанные в это поле данные для всех активов.
   - Вы можете изменить значения параметров полей. При изменении значения по умолчанию уже записанные в поля активов данные не меняются.
   - Чтобы изменить порядок отображения полей, используйте кнопки **Вверх** и **Вниз**.

5. Нажмите на кнопку **Сохранить**.

   Изменения внесены.

Активы критической информационной инфраструктуры

В OSMP можно помечать активы, относящиеся к критической информационной инфраструктуре (КИИ) Российской Федерации. Это позволяет ограничивать возможности пользователей OSMP по обращению с алертами и инцидентами, к которым относятся активы, относящиеся к объектам КИИ.

Присваивать активам КИИ-категорию можно, если в OSMP действует лицензия с модулем ГосСОПКА.

Присвоить активу КИИ-категорию могут Главные администраторы, а также пользователи, в профиле которых установлен флажок **Доступ к объектам КИИ**. Если ни одно из этих условий не выполнено, для пользователя действуют следующие ограничения:

- Не отображается блок параметров **Категория КИИ** в окнах **Информация об активе** и **Изменить актив**. Невозможно просмотреть или изменить КИИ-категорию актива.
- Не доступны для просмотра алерты и инциденты, к которым относятся активы с КИИ категорией. Над такими алертами и инцидентами невозможно производить никакие операции, в таблице алертов и инцидентов они не отображаются.
- Не отображается столбец **КИИ** в таблицах алертов и инцидентов.
- Недоступны операции поиска и закрытия алертов через REST API.

Категория КИИ актива отображается в окне **Информация об активе** в блоке параметров **Категория КИИ.**

Чтобы изменить КИИ-категорию актива:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** → **Обнаружение и реагирование**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив и нажмите **Сведения**.

   Откроется окно **Информация об активе**.
4. Нажмите на кнопку **Изменить** и в раскрывающемся списке выберите одно из доступных значений:
   - **Информационный ресурс не является объектом КИИ** – значение по умолчанию, которое означает, что у актива нет категории КИИ. С таким активом, а также с алертами и инцидентами, к которым относится этот актив, могут взаимодействовать пользователи, у которых в профиле не установлен флажок **Доступ к объектам КИИ**.
   - **Объект КИИ без категории значимости**.
   - **Объект КИИ третьей категории значимости**.
   - **Объект КИИ второй категории значимости**.
   - **Объект КИИ первой категории значимости**.
5. Нажмите на кнопку **Сохранить**.

Развертывание приложений "Лаборатории Касперского"

В этом разделе описано, как развернуть приложения "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью OSMP Console.

Сценарий: развертывание приложений "Лаборатории Касперского"

В этом сценарии описана процедура развертывания приложений "Лаборатории Касперского" с помощью Консоли OSMP. Можно воспользоваться мастером развертывания защиты или выполнить все необходимые шаги вручную.

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Загрузка и создание инсталляционных пакетов**

   Загрузите пакет вручную.

   Если вы не можете установить приложения "Лаборатории Касперского" с помощью Kaspersky EDR Expert на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты для приложений. Если вы используете автономные пакеты для установки приложений "Лаборатории Касперского", вам не нужно создавать и запускать задачу удаленной установки, а также создавать и настраивать задачи для Kaspersky Endpoint Security для Windows.

   Также можно загрузить дистрибутивы Агента администрирования и приложений безопасности с сайта "Лаборатории Касперского". Если удаленная установка приложений по каким-либо причинам невозможна, вы можете использовать загруженные дистрибутивы для локальной установки приложений.

2. **Создание, настройка и запуск задачи удаленной установки**

   Этот шаг входит в мастер развертывания защиты. Если вы не запускали мастер развертывания защиты, вам необходимо создать и настроить эту задачу вручную.

   Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одного приложения в этих задачах.

   Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

   > Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

3. **Создание и настройка задач**

   Задача *Обновление* Kaspersky Endpoint Security должна быть настроена.

   Создайте эту задачу вручную и настройте ее. Убедитесь, что расписание запуска задачи соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

4. **Создание политик**

   Создайте политику для Kaspersky Endpoint Security вручную. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры политики в соответствии с вашими требованиями.

5 **Проверка результатов**

Убедитесь, что развертывание завершилось успешно: созданы политики и задачи для каждого приложения и эти приложения установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Мастер развертывания защиты

Для установки приложений "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку приложений как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет находится в разделе **Управление программным обеспечением** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

Шаг 1. Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

Чтобы запустить мастер развертывания защиты вручную,

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 2. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

Шаг 3. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

  Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

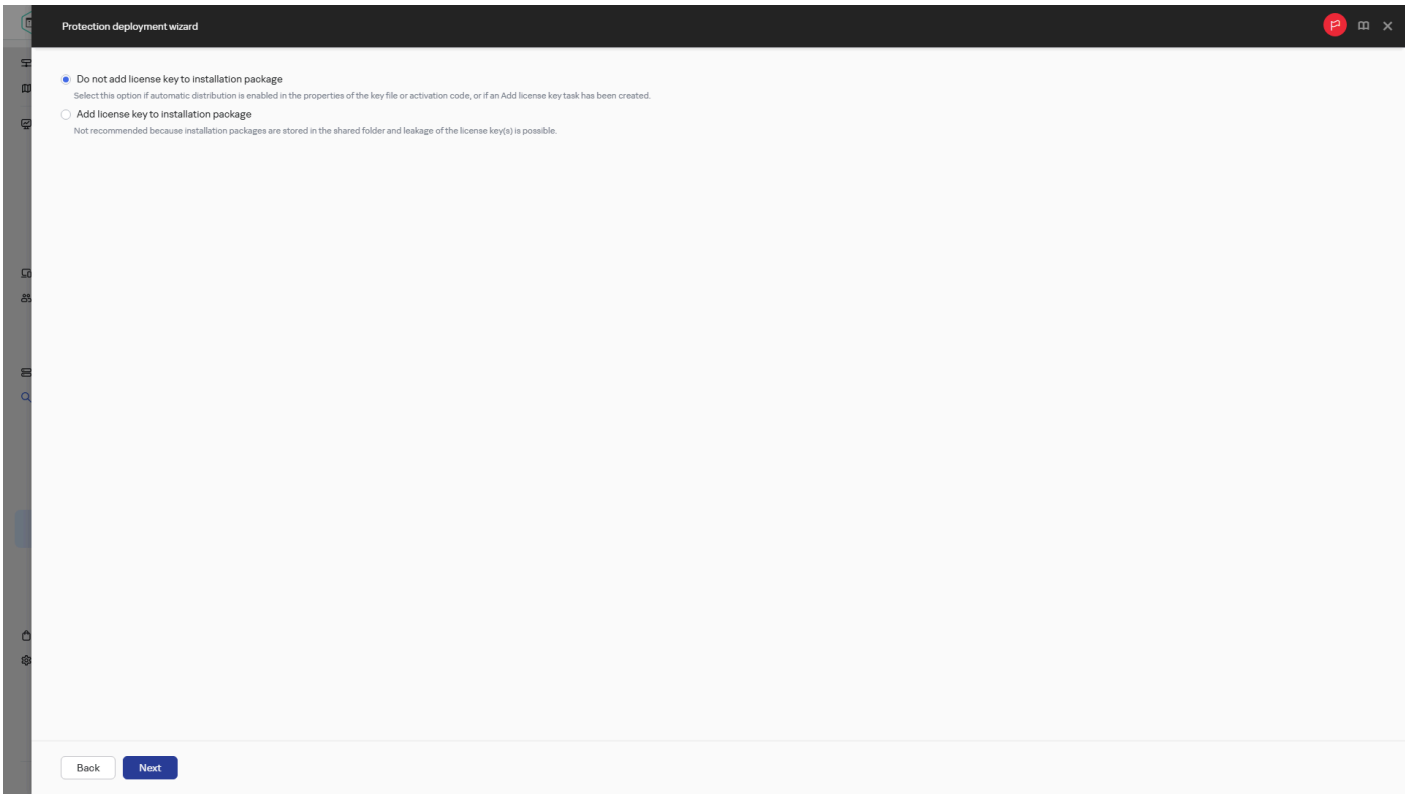
  - если в свойствах ключа настроено автоматическое распространение;
  - если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

  Ключ распространяется на устройства вместе с инсталляционным пакетом.

  > Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только информацию о лицензионном ключе.

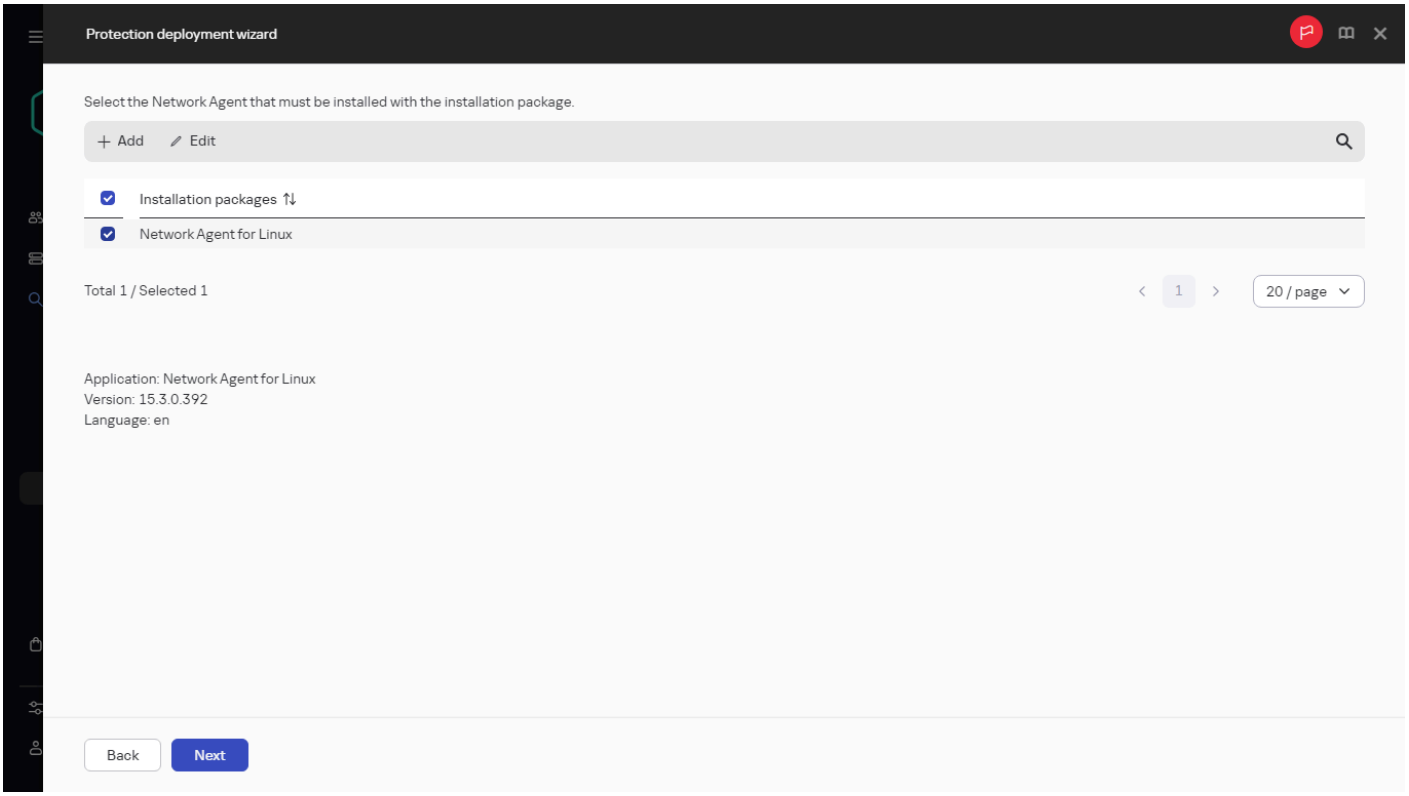


Выбор способа распространения файла ключа или кода активации

Шаг 4. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличный от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования.

Выберите последнюю версию Агента администрирования.



Выбор версии Агента администрирования

Шаг 5. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

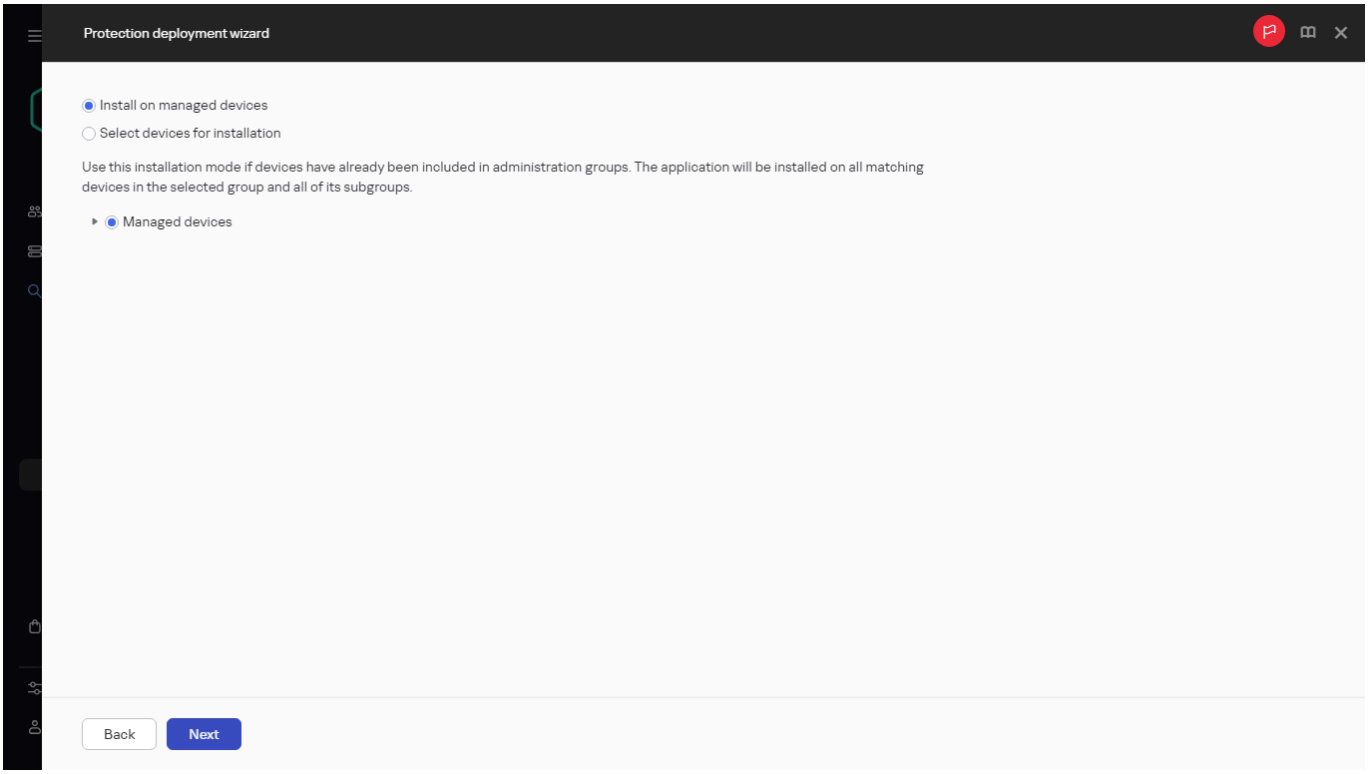
- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.



Указание устройств, на которые будет установлено приложение

Шаг 6. Задание параметров задачи удаленной установки

В окне **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно скачать инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

  Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

  По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

  Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

- Выберите этот параметр.
- Убедитесь, что для целевых клиентских устройств назначена точка распространения.
- Убедитесь, что на точке распространения установлена операционная система Windows.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

Настройте дополнительный параметр:

- **Не устанавливать приложение, если оно уже установлено**

  Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

  Если этот параметр выключен, приложение будет установлено в любом случае.

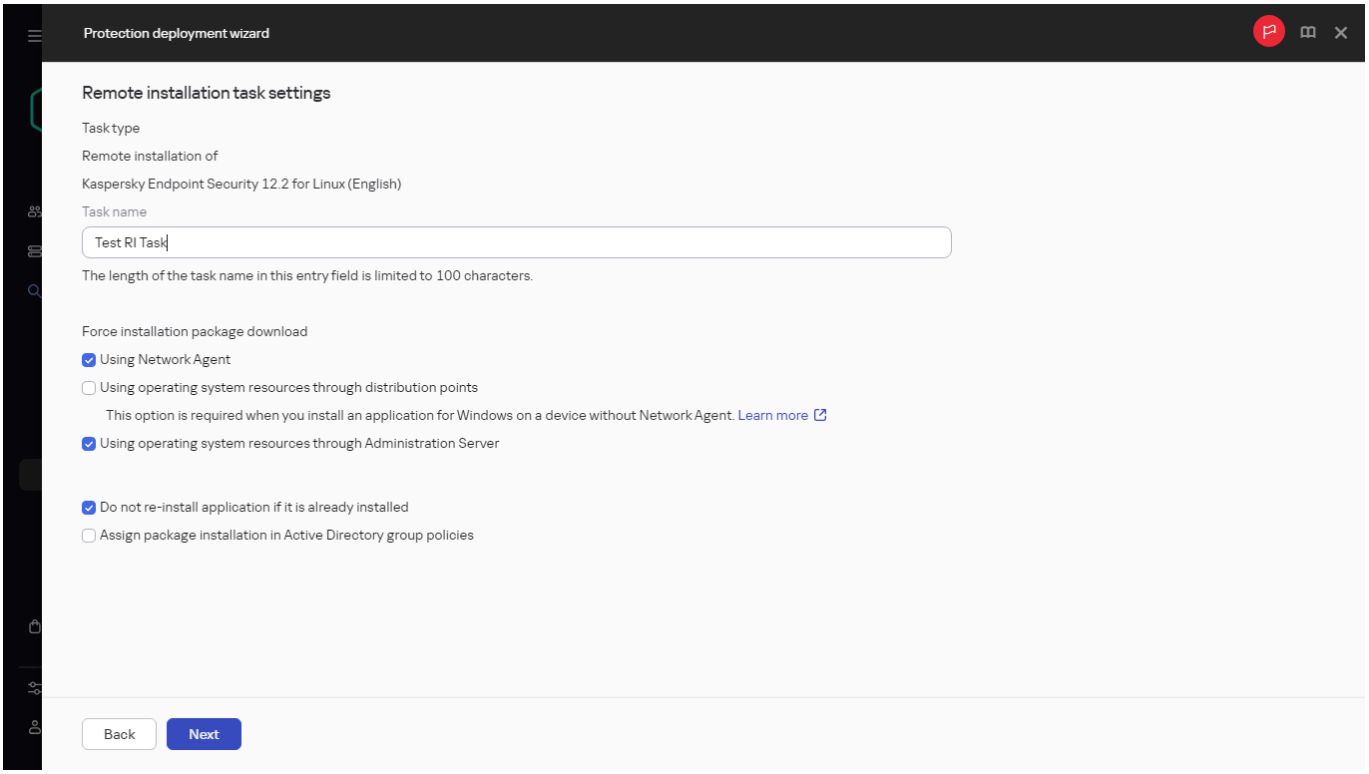
  По умолчанию параметр включен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

По умолчанию параметр выключен.



Задание параметров задачи удаленной установки

Шаг 7. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки приложения:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

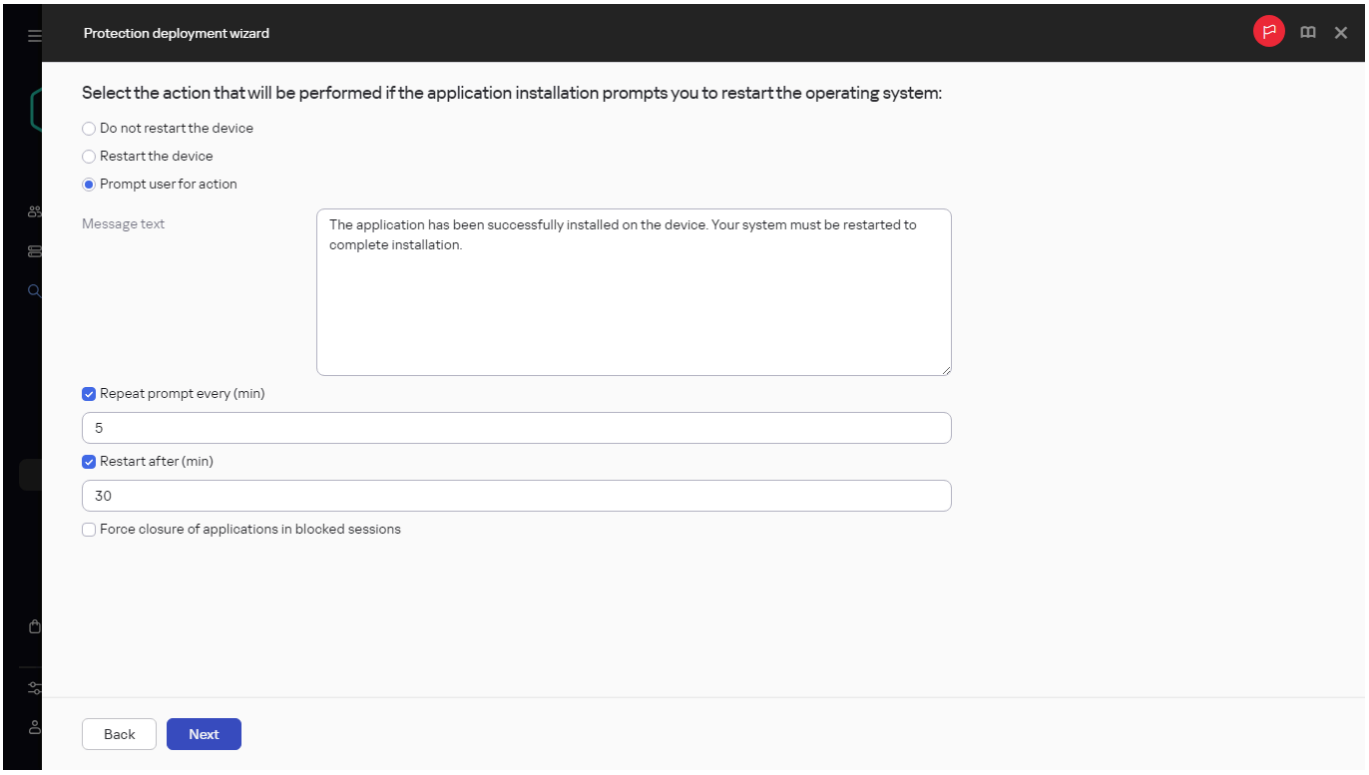
- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.



Указание параметра перезагрузки операционной системы

Шаг 8. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Kaspersky EDR Expert автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

Шаг 9. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

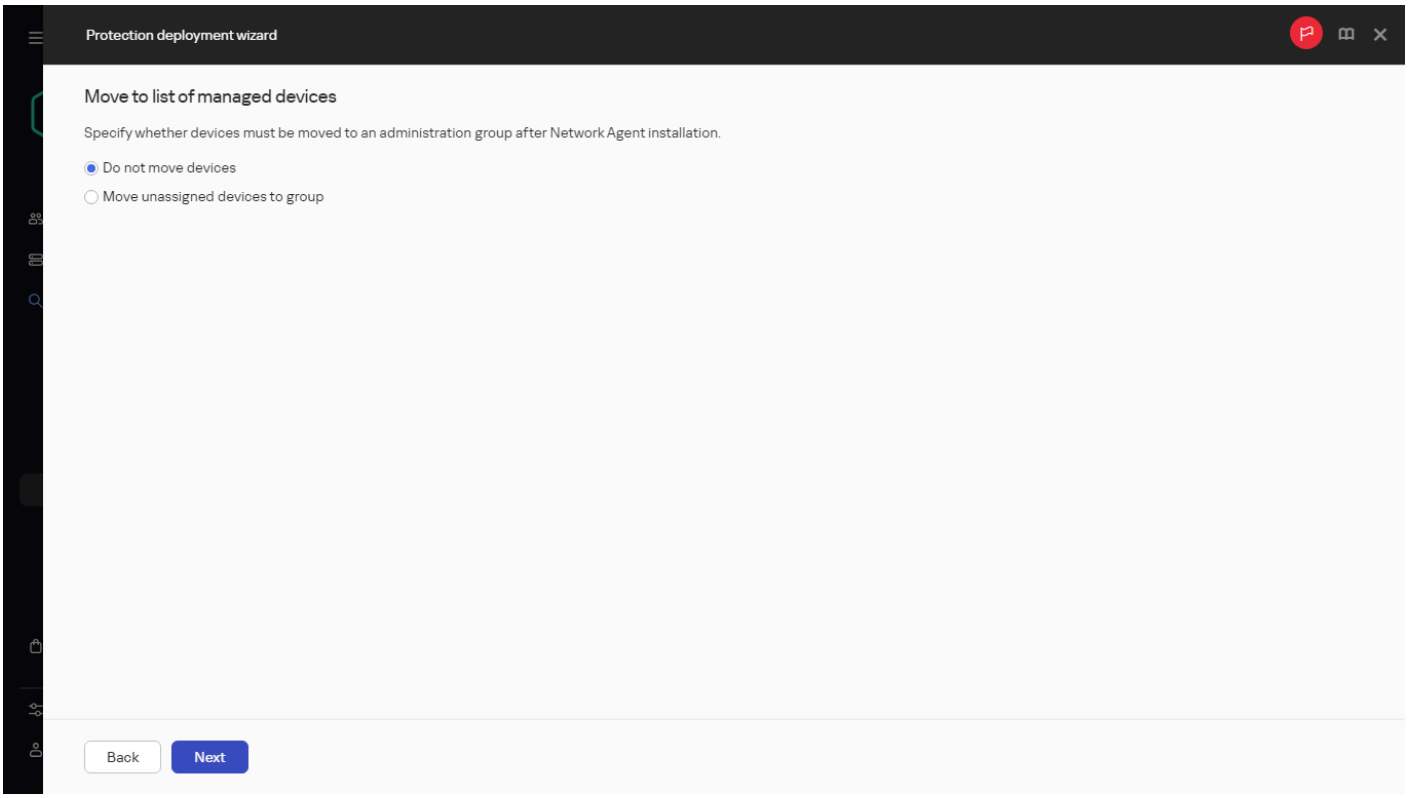
- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Перемещать нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.



Выбор варианта перемещения устройств в группу администрирования

Шаг 10. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для установки приложения.

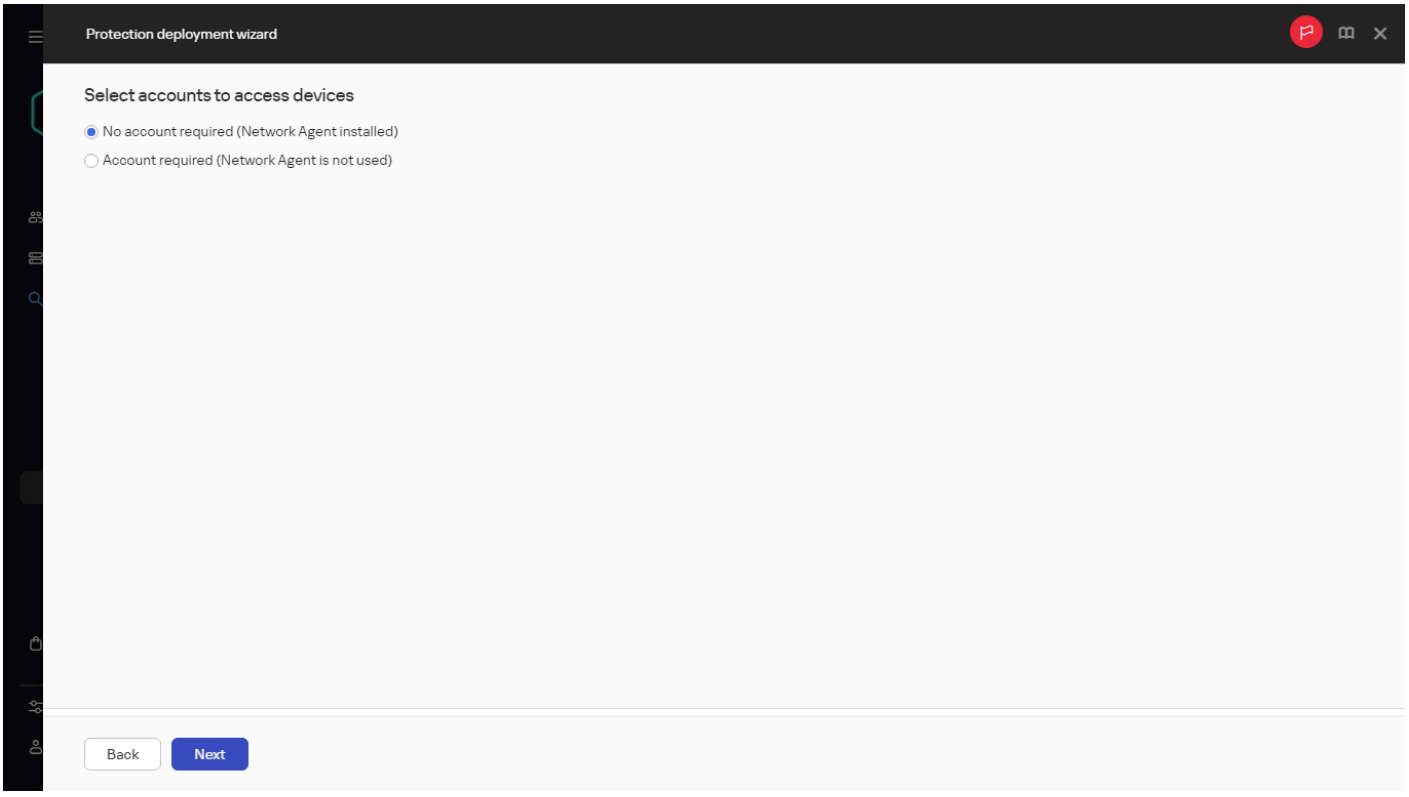
  - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите данные учетной записи пользователя.

    Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

- **SSH сертификат**. Если вы хотите установить приложение на клиентское устройство под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

  Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Open Single Management Platform поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Open Single Management Platform. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
  ```



Выбор учетных записей для доступа к устройствам

Шаг 11. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки приложения** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки приложения** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки приложения** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **OK**, чтобы завершить последний шаг мастера развертывания защиты.

Добавление плагина управления для приложений "Лаборатории Касперского"

Для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP необходимо использовать веб-плагины управления. Веб-плагины управления устанавливаются автоматически после развертывания Kaspersky EDR Expert.

Если вам необходимо вручную переустановить веб-плагин, обратитесь в Службу технической поддержки "Лаборатории Касперского", чтобы получить архив с нужным плагином управления.

Чтобы переустановить веб-плагин управления для приложения "Лаборатории Касперского":

1. Переместите архив веб-плагина управления на устройстве администратора, на котором расположена утилита KDT.

2. При необходимости экспортируйте текущую версию конфигурационного файла на устройстве администратора.

   Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.

3. Выполните команду, чтобы установить плагин:

   ```
   ./kdt apply -k <path_to_plugin_archive> -i <path_to_configuration_file>
   ```

   В команде укажите путь к архиву плагина и путь к текущему конфигурационному файлу. Если параметры установки не добавлены или не изменены, вам не нужно указывать путь к конфигурационному файлу в команде.

Веб-плагин управления переустановлен. Перезагрузите Консоль OSMP, чтобы плагин обновился.

Вы можете просмотреть список компонентов, относящихся к OSMP (включая веб-плагины управления), с помощью KDT. Также вы можете просмотреть версию Консоли OSMP и список установленных веб-плагинов управления. Для этого в верхней панели Консоли OSMP перейдите в меню своей учетной записи и выберите пункт **О приложении**.

Удаление веб-плагина управления

Вы можете удалить веб-плагины управления приложениями "Лаборатории Касперского", которые предоставляют дополнительные возможности Kaspersky EDR Expert. Плагины служб Kaspersky EDR Expert используются для корректной работы Kaspersky EDR Expert и не могут быть удалены (например, плагин Incident Response Platform).

Чтобы удалить веб-плагин управления:

1. При необходимости выполните следующую команду, чтобы получить название плагина, который вы хотите удалить:

   ```
   ./kdt state
   ```

   Отобразится список компонентов.

2. На устройстве администратора выполните команду. Укажите название плагина, который вы хотите удалить:

```
./kdt remove --cnab <имя_плагина>
```

Указанный веб-плагин управления удален KDT.

Просмотр списка компонентов, интегрированных в Open Single Management Platform

Вы можете просмотреть список компонентов, интегрированы в OSMP (включая веб-плагины управления), с помощью KDT.

Чтобы просмотреть список компонентов,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt state
```

Список компонентов, интегрированных в OSMP (включая веб-плагины управления), отображается в окне командной строки.

Просмотр названий, параметров и пользовательских действий компонентов Kaspersky EDR Expert

KDT позволяет просматривать список компонентов Kaspersky EDR Expert, которые содержатся в транспортном архиве, а также список установленных компонентов. Также вы можете просмотреть список параметров и список настраиваемых действий компонента Kaspersky EDR Expert. Если для компонента доступны пользовательские действия, вы также можете просмотреть описание и параметры указанного пользовательского действия с помощью KDT.

Пользовательское действие – это действие, позволяющее выполнять дополнительные операции, специфичные для компонента Kaspersky EDR Expert. Например, восстановление данных Сервера администрирования и увеличение объема дискового пространства, используемого Сервером администрирования и его журналом событий, выполняется с помощью пользовательских действий.

Пользовательское действие запускается с помощью KDT следующим образом:

```
./kdt invoke <название_компонента> --action <пользовательское_действие> --param
<парметр_пользовательского_действия>
```

Чтобы просмотреть список компонентов Kaspersky EDR Expert, включенных в транспортный архив,

на устройстве администратора, на котором расположена утилита KDT, выполните команду. В команде укажите путь к транспортному архиву и его название:

```
./kdt describe -k <название_транспортного_архива_и_путь>
```

Чтобы просмотреть список компонентов Kaspersky EDR Expert,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt describe
```

Отобразится список компонентов Kaspersky EDR Expert.

Чтобы просмотреть список параметров и список пользовательских действий компонента Kaspersky EDR Expert,

на устройстве администратора, на котором расположена утилита KDT, выполните команду и укажите имя компонента Kaspersky EDR Expert:

```
./kdt describe <название_компонента>
```

Отображаются списки параметров и пользовательских действий, доступных для указанного компонента.

Чтобы просмотреть описание и список параметров настраиваемого действия,

на устройстве администратора, на котором расположена утилита KDT, выполните команду и укажите имя компонента Kaspersky EDR Expert и его команду:

```
./kdt describe <название_компонента> <название_действия>
```

Отображаются описание и список параметров пользовательского действия указанного компонента.

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создавать инсталляционные пакеты для приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского".

Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений. Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех приложений, которые совместимы с текущей версией Open Single Management Platform. По умолчанию в списке отображаются только приложения с языком, соответствующим языку интерфейса. Чтобы отобразить другие языки, нажмите **Фильтр** и настройте параметры фильтра.

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security for Linux.

   Откроется окно с информацией об инсталляционном пакете.

   > Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

5. Ознакомьтесь с информацией и нажмите на кнопку **Скачать и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Скачать и создать инсталляционный пакет** отображается кнопка **Скачать дистрибутив**.

   Начинается загрузка инсталляционного пакета на Сервер администрирования. Вы можете закрыть окно мастера. В этом случае процесс скачивания продолжится в фоновом режиме. Вы можете отслеживать статус загрузки инсталляционного пакета, а также фильтровать и сортировать статусы в столбце **Статус инсталляционного пакета**.

   Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и перейдите к шагу 6 этой инструкции. По умолчанию инсталляционные пакеты со статусами **В процессе** и **Принять Лицензионное соглашение** располагаются в начале списка.

   > Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. Во время процесса загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

   a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение (EULA).

   b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.

      Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

7. После завершения загрузки нажмите на кнопку **Закрыть**.

Инсталляционный пакет отображается в списке инсталляционных пакетов.

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет.

Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

Чтобы создать пользовательский инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет из файла**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

5. В открывшемся окне выберите файл архива, расположенный на доступных дисках.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.

   Начнется загрузка файла на Сервер администрирования.

6. Если вы указали файл приложения "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение для этого приложения. Чтобы продолжить, вам нужно принять условия Лицензионного соглашения. Выберите параметр **Принять условия и положения настоящего Лицензионного соглашения**, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

   Также вам будет предложено прочитать и принять условия Политики конфиденциальности. Чтобы продолжить, вам нужно принять условия Политики конфиденциальности. Выберите параметр **Я принимаю Политику конфиденциальности**, только если вы понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.

7. Выберите файл (из списка файлов, которые извлечены из выбранного архивного файла) и укажите параметры командной строки исполняемого файла.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   Начнется процесс создания инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

8. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя**. Название инсталляционного пакета.
  - **Статус инсталляционного пакета**. Статус скачивания инсталляционного пакета.
  - **Источник**. Имя поставщика приложения.
  - **Приложение**. Название приложения, упакованного в пользовательский инсталляционные пакет.
  - **Версия**. Версия приложения.
  - **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **ОС**. Тип операционной системы, для которой предназначен инсталляционные пакет.
  - **Создано**. Дата создания инсталляционного пакета.
  - **Изменено**. Дата изменения инсталляционного пакета.
  - **Тип**. Тип инсталляционного пакета.
- Измените параметры командной строки.

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky EDR Expert. Вы можете создать автономный инсталляционный пакет для приложений "Лаборатории Касперского", так и для приложений сторонних производителей. Чтобы создать автономный инсталляционный пакет для приложений стороннего производителя, необходимо создать пользовательский инсталляционный пакет.

Если Сервер администрирования имеет доступ в интернет, для загрузки зависимостей, необходимых для создания автономных инсталляционных пакетов Агента администрирования, используется задача **Загрузка обновлений в хранилище Сервера администрирования**. Если у Сервера администрирования нет доступа в интернет, выполните следующие действия:

1. Выполните следующую команду, чтобы создать флаг RIUtilsArchiveDirUsed:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Выполните следующую команду, чтобы перезапустить службу Сервера администрирования:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Скачайте следующие архивы с сайта "Лаборатории Касперского" и поместите их в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

Теперь у Сервера администрирования есть нужные зависимости.

Убедитесь, что автономный инсталляционный пакет не доступен для третьих лиц.

Чтобы создать автономный инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

3. Выберите параметр **С использованием автономного инсталляционного пакета**.

   Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

   Параметр отображается в зависимости от приложения, для которого вы создаете автономный инсталляционный пакет.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.

- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, не изменяйте этот параметр.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

6. После завершения процесса создания автономного инсталляционного пакета, нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создается и размещается на Веб-сервере. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
MaxArchivePkgSize -t d -v < количество байтов >'
```

Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
MaxArchivePkgSize -t d -v 2147483648'
```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)

Вы можете установить Агент администрирования на устройства с операционной системой Linux с помощью файла ответов – текстового файла, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя.

Перед установкой Агента администрирования на устройство с операционной системой Linux нужно выполнить общие подготовительные шаги, которые требуются для всех Linux-устройств.

После выполнения общих шагов вы можете выполнить дополнительные инструкции, в соответствии с вашей операционной системой:

- Подготовка устройства с операционной системой SUSE Linux Enterprise Server 15.
- Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды.
- Подготовка устройства с операционной системой Ubuntu Server/Desktop версий 10.04 и 16.04.
- Подготовка устройства с операционной системой Linux с glibc 2.5.

Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Создайте файл ответов (в формате TXT). Добавьте в файл ответов список переменных в формате VARIABLE_NAME=variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вам нужно включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В таблице ниже перечислены все переменные, которые можно включать в файл ответов:

   Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_SERVER	Да	Содержит имя Сервера администрирования, представленное как полное доменное имя (FQDN) или IP-адрес.	DNS-имя устройства или IP-адрес.
KLNAGENT_AUTOINSTALL	Да	Определяет, включен ли тихий режим установки.	1 – тихий режим включен; пользователю не предлагается никаких действий во время установки. Другое – тихий режим выключен; пользователю могут быть предложены действия во время установки.
EULA_ACCEPTED	Да	Определяет, принимает ли пользователь Лицензионное соглашение Агента администрирования; если переменная не указана это может быть истолковано как отклонение Лицензионного соглашения.	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. Другое значение или не задано – Я не согласен с условиями Лицензионного соглашения (установка не выполняется).
KLNAGENT_PROXY_USE	Нет	Определяет, будет ли соединение с Сервером администрирования использовать параметры прокси-сервера. По умолчанию указано значение 0.	1 – используются параметры прокси-сервера. Другое – параметра прокси-сервера не используются.
KLNAGENT_PROXY_ADDR	Нет	Определяет адрес прокси-сервера, используемого для соединения с Сервером администрирования.	DNS-имя устройства или IP-адрес.
KLNAGENT_PROXY_LOGIN	Нет	Определяет имя пользователя, используемое для входа на прокси-сервер.	Любое существующее имя пользователя.
KLNAGENT_PROXY_PASSWORD	Нет	Определяет пароль пользователя, используемый для входа на прокси-сервер.	Любой набор букв и цифр, разрешенных форматом пароля в операционной системе.
KLNAGENT_VM_VDI	Нет	Определяет, установлен ли Агент администрирования на образ для создания динамических виртуальных машин.	1 – Агент администрирования установлен на образ, который затем будет использован для создания динамических виртуальных машин. Другое – во время установки образ не используется.
KLNAGENT_VM_OPTIMIZE	Нет	Определяет, являются ли параметры Агента администрирования оптимальными для гипервизора.	1 – локальные параметры Агента администрирования по умолчанию изменены таким образом, что они позволяют оптимизировать использование на гипервизоре.
KLNAGENT_TAGS	Нет	Перечисляет теги, назначенные экземпляру Агента администрирования.	Один или несколько тегов, разделенных точкой с запятой.

KLNAGENT_UDP_PORT	Нет	Определяет UDP-порт, используемый Агентом администрирования. По умолчанию указано значение 15000.	Любой существующий номер порта.
KLNAGENT_PORT	Нет	Определяет порт (не TLS), используемый Агентом администрирования. По умолчанию указано значение 14000.	Любой существующий номер порта.
KLNAGENT_SSLPORT	Нет	Определяет TLS-порт, используемый Агентом администрирования. По умолчанию указано значение 13000.	Любой существующий номер порта.
KLNAGENT_USESSL	Нет	Определяет, используется ли безопасность транспортного уровня (TLS) для подключения.	1 (по умолчанию) – используется TLS. Другое – TLS не используется.
KLNAGENT_GW_MODE	Нет	Определяет, используется ли шлюз соединения.	1 (по умолчанию) – текущие параметры не изменяются (при первом вызове шлюз соединения не указывается). 2 – шлюз соединения не используется. 3 – используется шлюз соединения. KLNAGENT_GW_ADDRESS – обязательный параметр. 4 – экземпляр Агента администрирования используется в качестве шлюза соединения в демилитаризованной зоне (DMZ). Требуется сертификат Сервера.
KLNAGENT_GW_ADDRESS	Нет	Определяет адрес шлюза соединения. Значение применимо, только если KLNAGENT_GW_MODE=3.	DNS-имя устройства или IP-адрес.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. Другое – выключено.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Нет	Определяет, устанавливать ли автоматически загруженные обновления для Агента администрирования со статусом *Не определено*.	true (по умолчанию) – обновления устанавливаются автоматически. false – обновления приложения не устанавливаются автоматически.

3. Запустите инсталляционный пакет Агент администрирования. Переменная среды KLAUTOANSWERS, указывающая путь к файлу ответов, передается в команде для установки. Выполните одну из следующих команд:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent-<номер сборки>.i386.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent64-<номер сборки>.x86_64.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent64-<номер сборки>.aarch64.rpm`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent_<номер сборки>_i386.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent64_<номер сборки>_amd64.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent64_<номер сборки>_arm64.deb`

   В зависимости от конфигурации операционной системы вы также можете использовать менеджеры пакетов rpm, dpkg или dnf для установки Агента администрирования.

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

Выполните команды, представленные в этой инструкции, под учетной записью root.

Чтобы подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:

1. Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите следующие параметры:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. В командной строке введите следующую команду, чтобы установить пакет совместимости:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Создайте директорию для ключа приложения:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Поместите ключ приложения /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg в директорию, созданную на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Если в комплект поставки Open Single Management Platform не входит ключ kaspersky_astra_pub_key.gpg, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

Linux-устройство готово к установке Агента администрирования. Вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:

Нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенного в пакет.
- **Название приложения**. Имя приложения, которое включено в автономный инсталляционный пакет.
- **Версия приложения**.
- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.

- **Размер**. Размер файла (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Путь**. Полный путь к папке, в которой находится автономный инсталляционный пакет.
- **Веб-адрес**. Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла**. Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

Информация о размере файла, хеше файла и пути отсутствует в списке инсталляционных пакетов для автономного пакета Агента администрирования, а также для пакетов, созданных на виртуальных Серверах администрирования. Эти автономные инсталляционные пакеты генерируются во время загрузки.

Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.
- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Скачать**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Open Single Management Platform позволяет вам создавать инсталляционные пакеты для приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку приложений на свои клиентские устройства.

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.

2. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

4. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите название задачи.

5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:

   - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.

   - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.

6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.

7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.

10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

Подготовка устройства с операционной системой Linux к установке Агента администрирования

Перед установкой Агента администрирования на Linux-устройство нужно выполнить подготовительные действия, необходимые для любого Linux-устройства.

Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.

2. Если вы хотите установить Агент администрирования на устройство с операционной системой Альт в режиме замкнутой программной среды, выключите режим замкнутой программной среды до завершения установки.

3. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса Web Console или с сайта "Лаборатории Касперского".

   Если вам необходимо установить Агент администрирования на устройство под управлением операционной системы Linux с glibc 2.5, вам нужно скачать инсталляционный пакет *Агент администрирования для устаревших версий Linux* с помощью интерфейса Web Console или с сайта "Лаборатории Касперского".

4. Убедитесь, что на целевом устройстве с операционной системой Linux установлено следующее программное обеспечение:

   - Sudo (для Ubuntu 10.04, версия Sudo 1.7.2p1 или выше).
   - Интерпретатор языка Perl версии 5.10 или выше.
   - Утилита ps.

5. Выполните проверку конфигурации устройства:

   a. Проверьте, что возможно подключение к устройству через SSH (например, приложение PuTTY).

      Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

      ```
      PasswordAuthentication no
      ```

      ```
      ChallengeResponseAuthentication yes
      ```

Не изменяйте файл /etc/ssh/sshd_config, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

b. Убедитесь, что порт TCP 22 открыт и доступен на нераспределенном устройстве с операционной системой Linux.

   Для успешной установки Агента администрирования для Linux должен быть доступен TCP-порт 22.

c. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

d. Используйте команду `visudo`, чтобы открыть конфигурационный файл sudoers.

   В открывшемся файле добавьте следующую строку в конец файла: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<имя пользователя>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Сохраните и закройте файл sudoers.

f. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

6. Если вы хотите удаленно установить Агент администрирования на устройствах с операционной системой с системой инициализации systemd, откройте файл `/etc/systemd/logind.conf` и выполните одно из следующих действий:

   - Укажите значение `no` для параметра `KillUserProcesses`: `KillUserProcesses=no`.
   - Для параметра `KillExcludeUsers` введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

   Целевое устройство Astra Linux

   Если целевое устройство работает под управлением Astra Linux, добавьте строку `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<имя пользователя>/.bashrc`, где `<имя пользователя>` – учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

   Целевое устройство ОСнова

   Если на целевом устройстве работает ОСнова, выполните следующие действия:

   a. Откройте файл `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` и закомментируйте строку `#KillUserProcess=yes`.

   b. Откройте файл `/usr/lib/NESS/pam-user-session` и закомментируйте строку `#loginctl terminate-session "$XDG_SESSION_ID"`.

   Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
sudo systemctl restart systemd-logind.service
```

7. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

8. Если вы хотите установить Агент администрирования на устройства с операционной системой Astra Linux, работающей в режиме замкнутой программной среды, выполните дополнительные действия для подготовки устройств Astra Linux.

9. Если вы хотите установить Агент администрирования на устройствах под управлением Ubuntu Server или Ubuntu Desktop версии 10.04, выполните дополнительные шаги для подготовки этих устройств.

10. Если вам нужно установить Агент администрирования на устройство под управлением операционной системы Linux с glibc 2.5, выполните дополнительную подготовку целевых устройств.

11. Если вы устанавливаете Агент администрирования на устройство с операционной системой Альт в режиме замкнутой программной среды, повторно включите режим закрытой программной среды.

12. Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 и выше или МСВСфера 9.2 и выше, установите пакет libxcrypt-compat для корректной работы Агента администрирования.

Linux-устройство готово к установке Агента администрирования. Вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Установка приложений с помощью задачи удаленной установки

Kaspersky EDR Expert позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку. Вы можете выбрать не более 1000 устройств.

Для того чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в разделе принудительного развертывания с помощью задачи удаленной установки Open Single Management Platform.

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными адресами или на выборку устройств.

Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

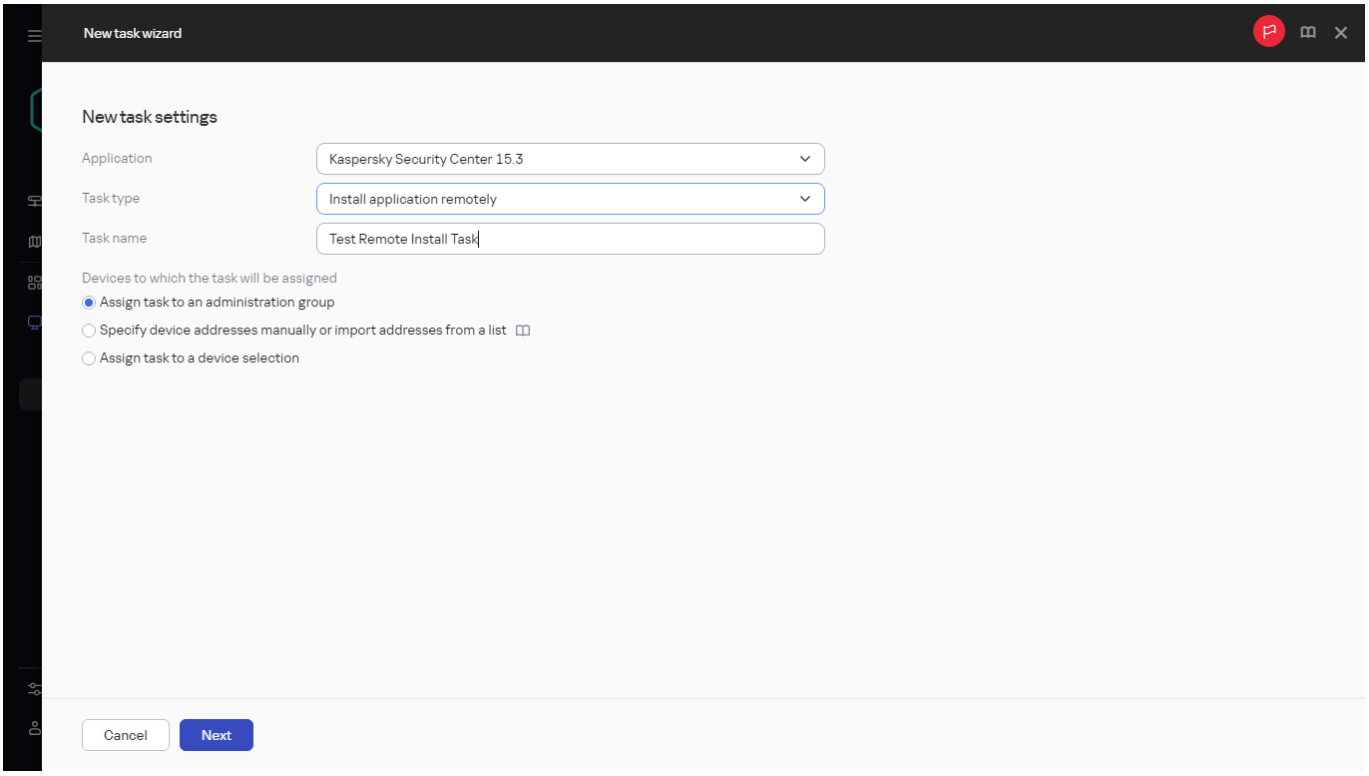
     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача *Удаленная установка приложения* создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.



Создание задачи Удаленная установка приложения

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   - В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.

   - В блоке параметров **Принудительно скачать инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

     - **С помощью Агента администрирования**

       Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

       Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

       Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

       По умолчанию параметр включен.

     - **Средствами операционной системы с помощью точек распространения**

       Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

- Выберите этот параметр.
- Убедитесь, что для целевых клиентских устройств назначена точка распространения.
- Убедитесь, что на точке распространения установлена операционная система Windows.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.

- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Open Single Management Platform больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другую, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

  Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно скачать инсталляционный пакет**.

  Вы можете использовать пароль деинсталляции только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security for Windows при установке Kaspersky Endpoint Security for Windows с помощью задачи Удаленная установка приложений. Использование пароля деинсталляции при установке других компонентов может вызвать ошибки установки.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center версии 15.1 для Windows или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:
  - **Не устанавливать приложение, если оно уже установлено**

    Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

    Если этот параметр выключен, приложение будет установлено в любом случае.

    По умолчанию параметр включен.

  - **Предварительно проверять тип операционной системы перед загрузкой**

    Перед передачей файлов на клиентские устройства Open Single Management Platform проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Open Single Management Platform не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

    При удаленной установке Агента администрирования на нераспределенные устройства Open Single Management Platform или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

  - **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

    Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

    Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

    По умолчанию параметр выключен.

  - **Предлагать пользователю закрыть работающие приложения**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

    Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

    По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:
  - **Устанавливать на все устройства**

    Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

    По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

  - **Устанавливать на устройства, управляемые только этим Сервером администрирования**

    Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.

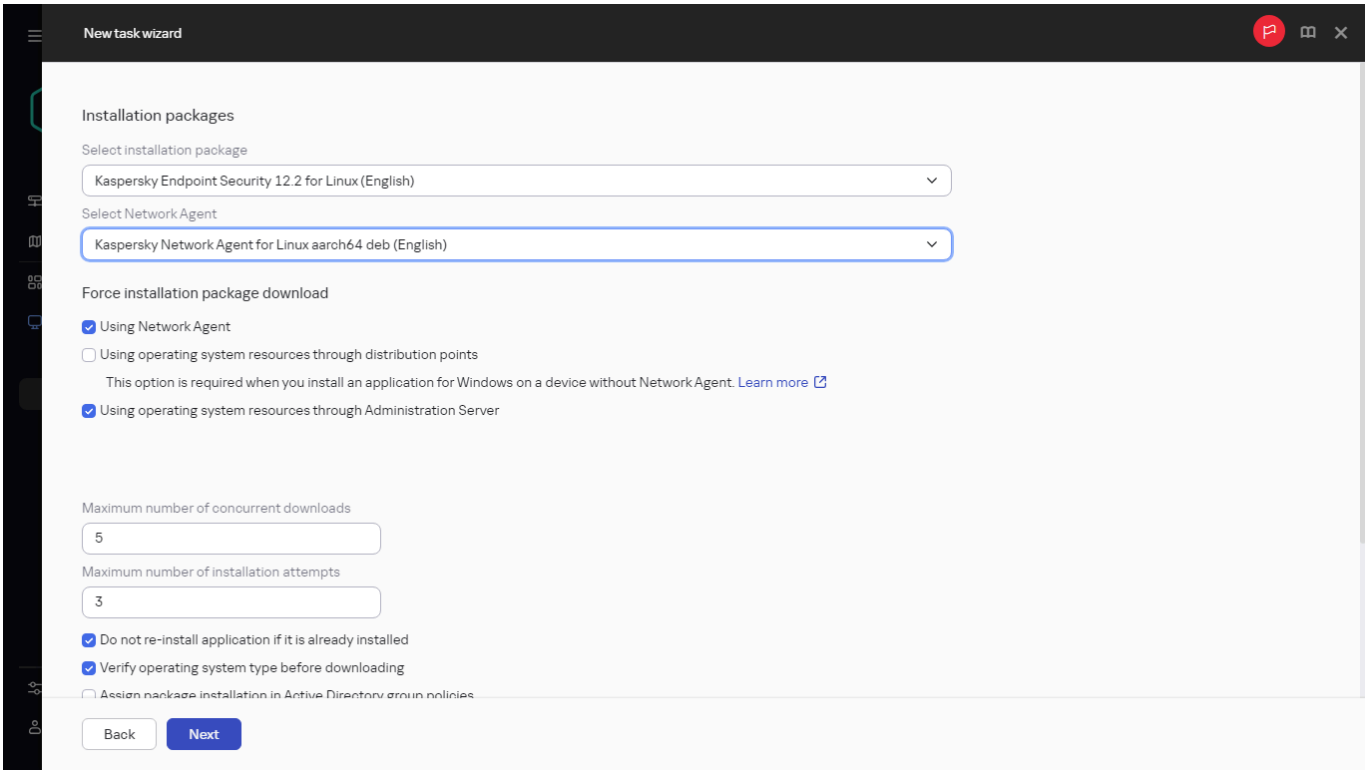
- Укажите, следует ли перемещать устройства в группу администрирования после установки:
  - **Не перемещать устройства**

    Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

  - **Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)**

    Устройства перемещаются в выбранную вами группу администрирования.

Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.



Указание параметров задачи

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки приложения безопасности.

   - **Перезагрузить устройство**

     Если выбран этот вариант, устройство будет перезагружено после установки приложения безопасности.

8. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка приложения*.

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   - **Учетная запись требуется (Агент администрирования не используется)**

     Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для установки приложения.

     - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите данные учетной записи пользователя.

       Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

     - **SSH сертификат**. Если вы хотите установить приложение на клиентское устройство под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

       Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Open Single Management Platform поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Open Single Management Platform. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
       ```

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

    Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранное приложение устанавливается на указанный набор устройств.

Установка приложений на подчиненные Серверы администрирования

Если у вас версия Сервера администрирования 15.4 или выше, вы можете устанавливать приложения на подчиненный Сервер администрирования только в том случае, если его версия 15.4 или выше.

Чтобы установить приложение на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.

3. Создайте задачу удаленной установки приложения на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранное приложение устанавливается на подчиненные Серверы администрирования.

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на название задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.

3. Перейдите в раздел **Параметры приложения** → **Параметры, специфичные для Unix**.

4. Задайте следующие параметры:

   Установить пароль для учетной записи root (только для развертывания через SSH)

Если команду `sudo` невозможно использовать на целевом устройстве без указания пароля, выберите этот параметр, а затем укажите пароль для учетной записи root. Kaspersky EDR Expert передает пароль в зашифрованном виде на целевое устройство, расшифровывает пароль, а затем запускает процедуру установки от имени учетной записи root с указанным паролем.

> Kaspersky EDR Expert не использует учетную запись или указанный пароль для создания SSH-соединения.

Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)

Если папка /tmp на целевом устройстве не имеет права Выполнение, выберите этот параметр, а затем укажите путь к папке с правами Выполнение. Kaspersky EDR Expert использует указанную папку в качестве временной папки для доступа по SSH. Приложение помещает инсталляционный пакет в директорию и запускает процедуру установки.

5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

Запуск и остановка приложений "Лаборатории Касперского"

Вы можете использовать задачу *Запуск или остановка приложения* для запуска и остановки приложений "Лаборатории Касперского" на управляемых устройствах.

Чтобы создать задачу запуска или остановки приложения:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите создать задачу.
4. В списке **Тип задачи** выберите задачу **Запуск и остановка приложения**.
5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.
7. В окне **Приложения** выполните следующее:
   - Установите флажки рядом с названиями приложений, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить приложение** или **Остановить приложение**.
8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на шаге **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями и сохраните параметры.

Задача создана и настроена.

Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Замещение приложений безопасности сторонних производителей

Для установки приложения безопасности "Лаборатории Касперского" средствами Kaspersky EDR Expert может потребоваться удалить приложение стороннего производителя, несовместимое с устанавливаемым приложением. Open Single Management Platform предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности в мастере развертывания защиты. Если этот параметр включен, Open Single Management Platform удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача *Удаленная деинсталляция приложения.* Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача *Удаленная деинсталляция приложения*.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Удаленная деинсталляция приложений или обновлений программного обеспечения

Вы можете удаленно деинсталлировать приложения или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

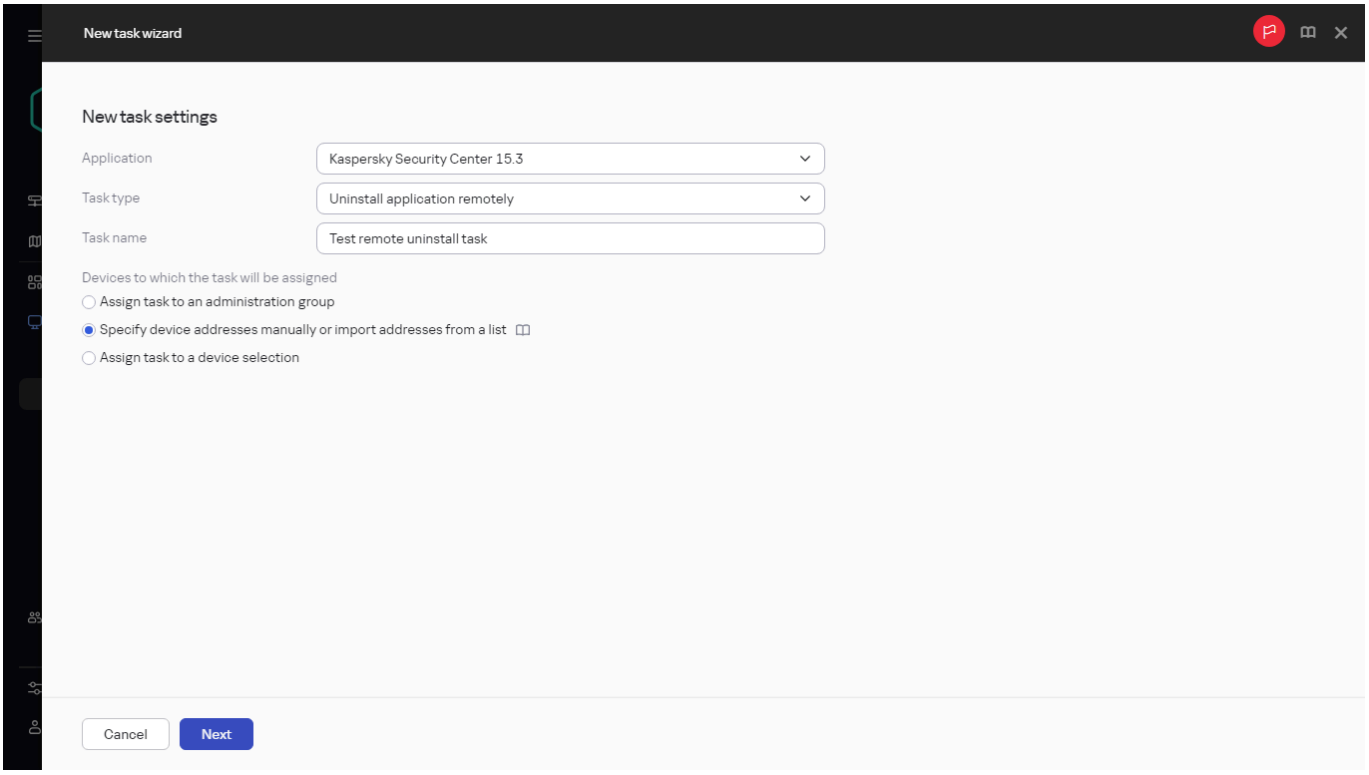
   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите Kaspersky EDR Expert.

4. В списке **Тип задачи** выберите тип задачи **Удаленная деинсталляция приложения**.

5. В поле **Название задачи** укажите название новой задачи.

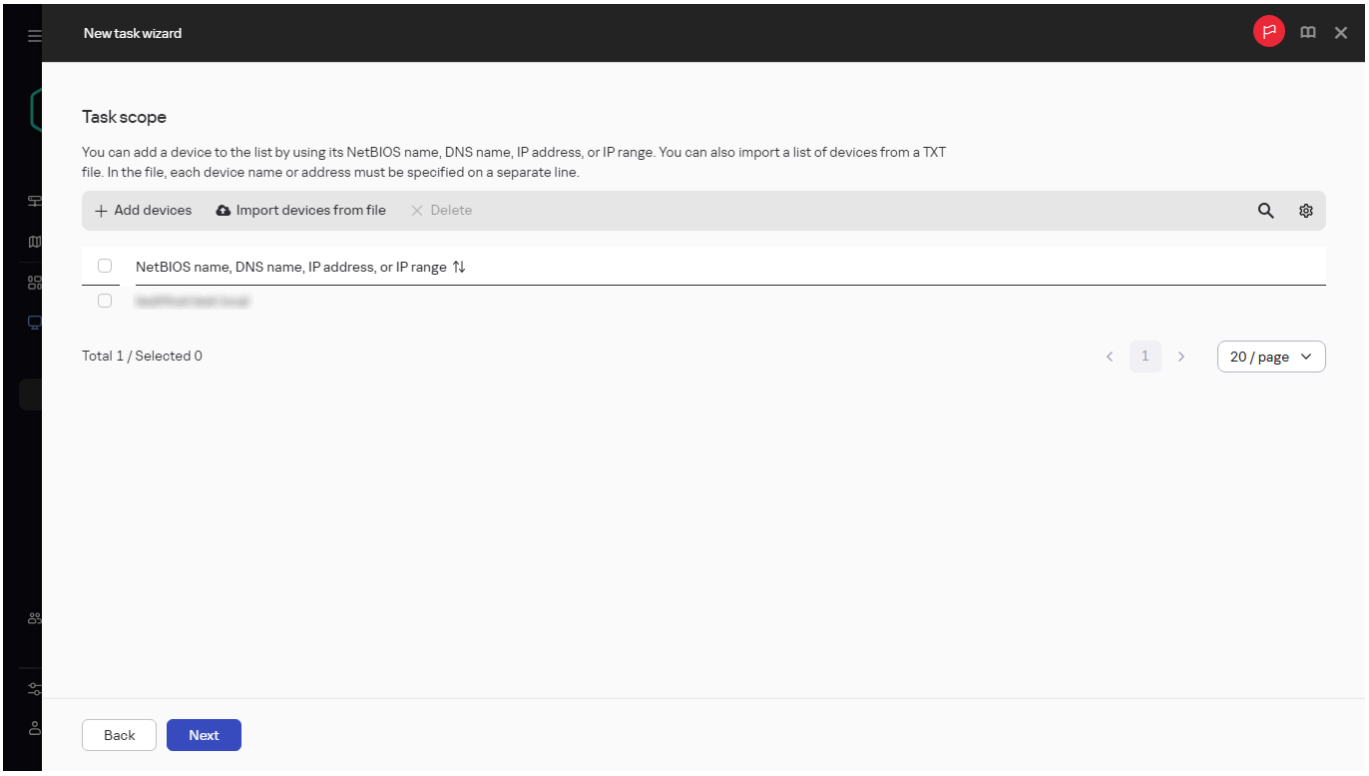
   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).



Создание задачи Удаленная деинсталляция приложения

6. Выберите устройства, которым будет назначена задача.

Перейдите к следующему шагу мастера.



Указание области действия задачи

7. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:

Удалить управляемое приложение

Отображается список приложений "Лаборатории Касперского". Выберите приложение, которое вы хотите деинсталлировать.

Убедитесь, что параметр политики **Использовать пароль деинсталляции** выключен для управляемого приложения.

Удалить несовместимое приложение

Отобразится список приложений, несовместимых с приложениями безопасности "Лаборатории Касперского" или с Open Single Management Platform. Установите флажки напротив приложений, которые требуется удалить.

Удалить приложение из реестра приложений

По умолчанию Агенты администрирования отправляют на Сервер администрирования информацию о приложениях, установленных на управляемых устройствах. Список установленных приложений хранится в реестре приложений.

Чтобы выбрать приложение из реестра приложений:

a. Нажмите на поле **Приложение для деинсталляции** и выберите приложение, которое вы хотите деинсталлировать.

> Если вы выбрали Агент администрирования Kaspersky Security Center, при запуске задачи статус *Завершено успешно* показывает, что процесс удаления запущен. При удалении Агента администрирования Kaspersky Security Center статус не меняется. В случае сбоя задачи статус меняется на *Сбой*.

b. Укажите параметры деинсталляции:

- **Способ удаления**

  Выберите, как вы хотите деинсталлировать приложение:

  - **Автоматически определять команду удаления**

    Если у приложения есть команда деинсталляции, заданная поставщиком приложения, Open Single Management Platform использует эту команду. Рекомендуется выбрать этот вариант.

  - **Задать команду удаления**

    Выберите этот вариант, если вы хотите указать свою команду для деинсталляции приложения.

    > Рекомендуется сначала попробовать деинсталлировать приложение с помощью параметра **Автоматически определять команду удаления**. Если деинсталляция с помощью автоматически определенной команды не удалась, используйте свою команду.

    Введите команду установки в это поле и укажите следующий параметр:

    Используйте эту команду для удаления, только если команда по умолчанию не была обнаружена автоматически

    Open Single Management Platform проверяет, есть ли у выбранного приложения команда деинсталляции, заданная поставщиком приложения. Если команда найдена, Open Single Management Platform будет использовать ее вместо команды, указанной в поле **Команда для удаления приложения**.

    Рекомендуется включать этот параметр.

- **Выполнить перезагрузку после успешного удаления приложения**

  Если после деинсталляции приложения требуется перезагрузка операционной системы на управляемом устройстве, операционная система перезагружается автоматически.

Удалить указанное обновление приложения, патч или стороннее приложение

Отображается список обновлений, патчей и приложений сторонних производителей. Выберите объект, который вы хотите деинсталлировать.

Отображаемый список представляет собой общий список приложений и обновлений, и он не соответствует приложениям и обновлениям, установленным на управляемых устройствах. Перед выбором объекта рекомендуется убедиться, что приложение или обновление установлено на устройствах, определенных в области действия задачи. В окне свойств можно просмотреть список устройств, на которых установлено приложение или обновление.

Чтобы просмотреть список устройств:

a. Нажмите на имя приложения или обновления.

   Откроется окно свойств.

b. Откройте раздел **Устройства**.

   Вы также можете просмотреть список установленных приложений и обновлений в окне свойств устройства.

8. Укажите, как клиентские устройства будут загружать утилиту удаления:

С помощью Агента администрирования

Файлы доставляются на клиентские устройства Агентом администрирования, установленным на этих клиентских устройствах.

Если этот параметр выключен, файлы доставляются с помощью инструментов операционной системы Linux.

Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

Средствами операционной системы с помощью Сервера администрирования

> Параметр устарел. Используйте параметр **С помощью Агента администрирования** или **Средствами операционной системы с помощью точек распространения** вместо этого параметра.

Файлы передаются на клиентские устройства с использованием средств операционной системы Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

Средствами операционной системы с помощью точек распространения

Файлы передаются на клиентские устройства с использованием инструментов операционной системы с помощью точек распространения. Этот параметр можно включить, если в сети есть хотя бы одна точка распространения.

Если параметр **С помощью Агента администрирования** включен, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

Максимальное количество одновременных загрузок

Максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы. Чем больше это число, тем быстрее будет деинсталлировано приложение, но нагрузка на Сервер администрирования увеличивается.

Максимальное количество попыток деинсталляции

Если при запуске задачи *Удаленная деинсталляция приложения* Open Single Management Platform не удается деинсталлировать приложение с управляемого устройства за указанное в параметрах количество запусков установок, Open Single Management Platform прекращает доставку утилиты деинсталляции на это управляемое устройство и больше не запускает установщик на устройстве.

Параметр **Максимальное количество попыток деинсталляции** позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует деинсталляции. Администратор должен решить проблему за указанное количество попыток деинсталляции и перезапустить задачу (вручную или по расписанию).

Если удаление не выполнено, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

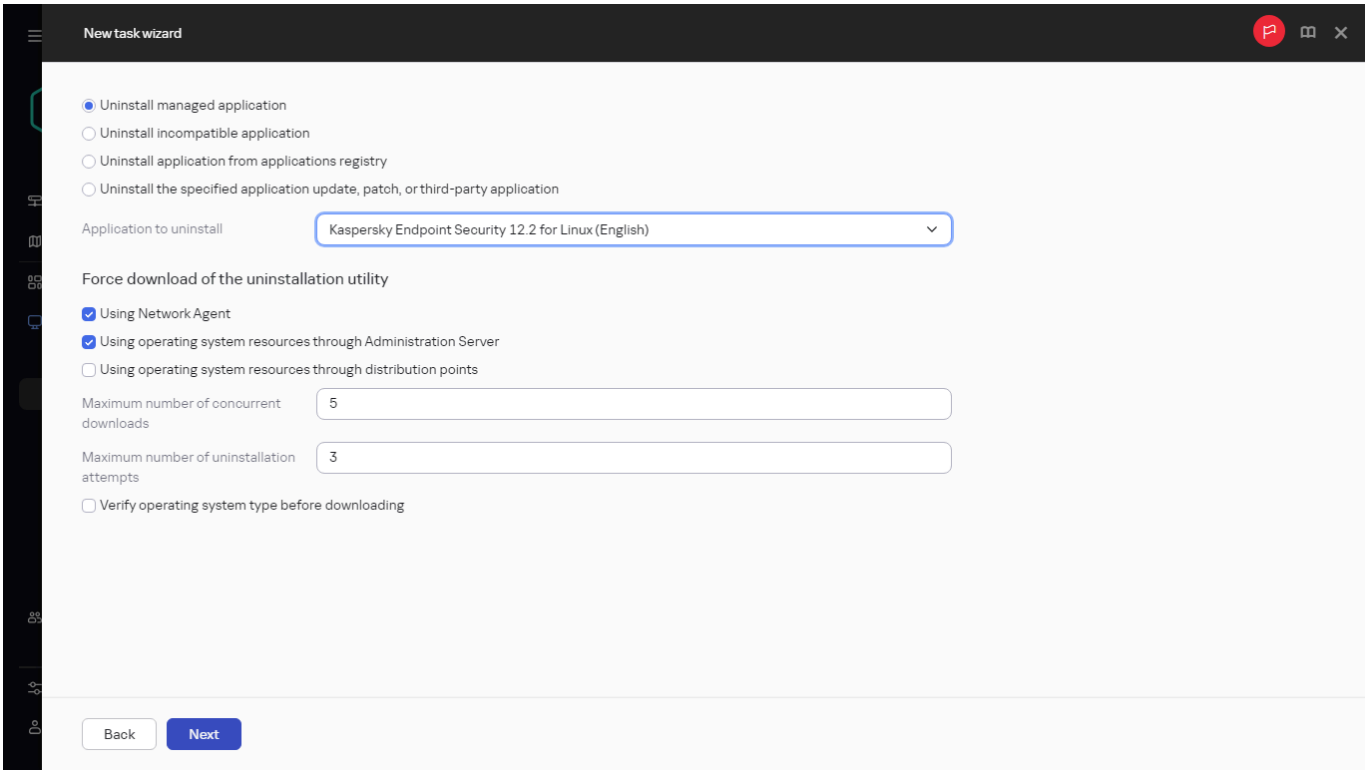
Если количество попыток деинсталляции, указанное в параметрах задачи, было превышено и устройство готово к деинсталляции приложения, вы можете увеличить значение параметра **Максимальное количество попыток деинсталляции** и запустить задачу деинсталляции приложения. Также вы можете создать другую задачу *Удаленная деинсталляция приложения*.

Предварительно проверять тип операционной системы перед загрузкой

Перед передачей файлов на клиентские устройства Open Single Management Platform проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Open Single Management Platform не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

При удаленной установке Агента администрирования на нераспределенные устройства Open Single Management Platform или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

Перейдите к следующему шагу мастера.



Указание параметров задачи

9. Укажите параметры перезагрузки операционной системы:

Не перезагружать устройство

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

Перезагрузить устройство

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

Запрашивать у пользователя

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**
- **Принудительно перезагрузить через (мин)**

Принудительно закрывать приложения в заблокированных сеансах

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

10. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

    Учетная запись не требуется (Агент администрирования уже установлен)

    Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

    Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

    Учетная запись требуется (Агент администрирования не используется)

    Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу *Удаленная деинсталляция приложения*. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для деинсталляции приложения.

    - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите данные учетной записи пользователя.

      Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

    - **SSH сертификат**. Если вы хотите деинсталлировать приложение с клиентского устройства под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Open Single Management Platform поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Open Single Management Platform. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen.

Например:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
```

11. Если на шаге мастера **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

    Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

12. Нажмите на кнопку **Готово**.

    В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо.

    > Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

    Задача будет создана, настроена и отобразится в списке задач в разделе **Задачи**.

13. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

    Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

    Подробное описание параметров запуска по расписанию см. в общих параметрах задачи.

После завершения задачи, выбранное приложение будет удалено на выбранных устройствах.

Ограничения удаленной деинсталляции

Иногда удаленная деинсталляция приложений сторонних производителей может завершится предупреждением: "Удаление на этом устройстве завершено с предупреждениями: Приложение для деинсталляции не установлено". Эта проблема возникает, когда приложение для деинсталляции, уже было деинсталлировано или было установлено только для одного пользователя. Приложения, установленные для одного пользователя (далее также "приложения для каждого пользователя"), становятся невидимыми и не могут быть деинсталлированы удаленно, если пользователь не вошел в систему.

Такое поведение отличается от поведения приложений, предназначенных для использования несколькими пользователями на одном устройстве (далее также "приложения устройства"). Приложения для каждого устройства видны и доступны всем пользователям этого устройства.

Поэтому приложения для каждого пользователя должны быть деинсталлированы только когда пользователь вошел в систему.

Источники информации об установленных приложениях

Агент администрирования получает информацию о программном обеспечении, установленном на устройствах Windows, из следующих ключей реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для текущего пользователя.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для набора пользователей.

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением SUSE Linux Enterprise Server 15 вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

Чтобы установить Агент администрирования на устройство с операционной системой SUSE Linux Enterprise Server 15:

перед установкой Агента администрирования выполните следующую команду:

```
sudo zypper install insserv-compat
```

Это позволит вам установить пакет insserv-compat и правильно настроить Агент администрирования.

Выполните команду `rpm -q insserv-compat`, чтобы проверить, если пакет уже установлен.

Если в вашей сети много устройств под управлением SUSE Linux Enterprise Server 15, вы можете использовать специальное программное обеспечение для настройки и управления инфраструктурой компании. Используя это программное обеспечение, вы можете автоматически установить пакет insserv-compat сразу на все необходимые устройства. Например, вы можете использовать Puppet, Ansible, Chef, или сделать свой скрипт любым удобным для вас способом.

Если на устройстве нет ключей подписи GPG для SUSE Linux Enterprise, вы можете увидеть следующее предупреждение: `Package header is not signed!` Select the `i` option to ignore the warning.

После подготовки Linux-устройства вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Подготовка устройства под управлением Windows к удаленной установке

Удаленная установка приложения на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве.

  В этом случае ее повторное выполнение не требуется.

- Во время запуска задачи устройство было выключено.

  В этом случае требуется включить устройство и запустить задачу еще раз.

- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве.

  Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).

- Если на устройстве не установлен Агент администрирования, при удаленной установке приложения могут возникнуть следующие ситуации:

  - Сетевые ошибки.
  - Неправильно настроенная операционная система.
  - Неправильно настроенные права учетной записи в задаче удаленной установки.

  Для того чтобы избежать проблем, которые могут возникнуть во время установки приложения на клиентское устройство без установленного Агента администрирования, вам нужно принудительно установить выбранные инсталляционные пакеты, используя задачу удаленной установки Open Single Management Platform при условии, что на каждом устройстве есть учетная запись (или учетные записи) пользователя с правами локального администратора.

Ранее использовалась утилита riprep для подготовки Windows-устройства к удаленной установке. Теперь это считается устаревшим способом настройки операционных систем. Утилиту riprep не рекомендуется использовать на операционных системах выше Windows XP и Windows Server 2003 R2.

Если устройства недоступны для Сервера администрирования напрямую, можно также использовать принудительную установку. Например, когда устройства находятся в изолированных сетях или в локальной сети, а Сервер администрирования находится в демилитаризованной зоне. В таких случаях нужна точка распространения для развертывания на этих устройствах.

Использование точек распространения в качестве локальных центров установки может быть удобно для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки невозможно выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью Сервера администрирования или точек распространения.

Вам нужно указать учетную запись, которая имеет доступ к общему ресурсу admin$, в параметрах задачи удаленной установки.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Open Single Management Platform, к которой они принадлежат, или создав выборку устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Принудительная установка осуществляется путем доставки инсталляционных пакетов на целевые устройства, последующего копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. Отправка инсталляционных пакетов на целевые устройства выполняется с помощью функции Open Single Management Platform, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Целевые устройства доступны с точки распространения с операционной системой Windows, с которой должна быть выполнена удаленная установка на клиентские устройства, и эта точка распространения выбрана для целевых устройств.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin$.
- На целевых устройствах запущены следующие системные службы:
  - Сервер (LanmanServer).

    По умолчанию эта служба запущена.
  - DCOM Server Process Launcher (DcomLaunch).
  - RPC Endpoint Mapper (RpcEptMapper).
  - Вызов удаленной процедуры (Remote Procedure Call, RpcSs).
- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментов Windows.

  TCP 139, UDP 137 и UDP 138 используются старыми протоколами и больше не нужны для текущих приложений.

  На сетевом экране должны быть разрешены динамические исходящие порты доступа для соединения точек распространения с целевыми устройствами.
- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTLM-протокола при развертывании Агента администрирования.
- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.

- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая – локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой – локальные пользователи выполняют аутентификацию как Гость*.

- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Для того чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

При установке на новые устройства, еще не размещенных в группах администрирования Open Single Management Platform, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Вы можете использовать несколько точек распространения для снижения нагрузки во время отправки инсталляционных пакетов на целевые устройства. Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Если вы используете точки распространения, вам нужно убедиться, что они присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Настройка приложений "Лаборатории Касперского"

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Создавайте и настраивайте политики и задачи, необходимые для вашей сети.

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования.
- Установили Консоль OSMP.
- Выполнили основной сценарий установки Open Single Management Platform.

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   В группе администрирования **Управляемые устройства** создайте вручную и настройте следующие политики и задачи:

   - политика Kaspersky Endpoint Security;
   - групповая задача обновления Kaspersky Endpoint Security;
   - политика Агента администрирования.

   Инструкции: Настройка групповой задачи обновления Kaspersky Endpoint Security.

   При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

3. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции: Настройка количества событий в хранилище событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства, позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с приоритетами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования и Консоль OSMP. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователей как альтернативу или дополнительную возможность для подхода, ориентированного на устройства. Узнайте больше о двух подходах к управлению.

Этапы

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

2. **Создание профилей политики (если требуется)**

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам с определенной конфигурацией программного обеспечения или с заданными теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *CentOS*, назначить его всем устройствам под управлением операционной системы CentOS, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы CentOS установленные приложения "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Создание профиля политики.
- Создание правила активации профиля политики.

3. **Распространение политик и профилей политик на управляемые устройства**

   По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования и Консоль OSMP и завершили основной сценарий развертывания. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению.

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующих пользователей.

   Инструкция: Назначение пользователя владельцем устройства.

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

   Инструкция: Создание роли пользователя.

5. **Определение области для каждой роли пользователя**

   Для каждой созданной роли пользователя определите пользователей и/или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

   Инструкция: Изменение области для роли пользователя.

6. **Создание профилей политики**

   Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите созданные профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: связь профилей политики с ролями.

8. **Распространение политик и профилей политик на управляемые устройства**

   По умолчанию синхронизация Open Single Management Platform с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на пользователя, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

О переключении Агента администрирования на другой Сервер администрирования

В Kaspersky EDR Expert предусмотрена возможность переключать Агент администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.

  Параметр **Условие для адреса DHCP-сервера** в настоящее время недоступен.

- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Условие для подсети** – изменение адреса и маски подсети.
- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с сервером (имя:порт). Используйте выделенный сервер с программным обеспечением, способным обрабатывать высокую нагрузку и частые запросы для подключения от Агента администрирования. Не указывайте порт Сервера администрирования. Для каждого сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат сервера в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.

- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.

- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

Создание профиля соединения для автономных пользователей

Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:

1. Если вы хотите создать профиль подключения для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

   b. Выберите группу администрирования, для которой нужно создать профиль соединения:

      - Для корневой группы вы можете перейти к следующему шагу.

      - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне нажмите на имя нужной подгруппы.

      Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

   c. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.

2. Если вы хотите создать профиль подключения для определенного управляемого устройства, выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   b. Нажмите на имя требуемого управляемого устройства.

   c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

   d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.

3. В открывшемся окне свойств перейдите в раздел **Параметры приложения** → **Подключения** → **Профили соединений.**

4. В разделе **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

   По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

   В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

   В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Настроить профиль** настройте параметры профиля подключения:

   - **Имя профиля**

     В поле ввода можно просмотреть или изменить имя профиля подключения.

   - **Адрес Сервера администрирования**

     Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

   - **Номер порта**

     Номер порта, по которому будет выполняться подключение.

   - **SSL-порт**

     Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

   - **Использовать SSL-соединение**

     Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

     По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

  - **Адрес**

    Адрес прокси-сервера для подключения Kaspersky EDR Expert к интернету.

  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky EDR Expert.

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  - **Имя пользователя**

    Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  - **Пароль**

    Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

- **Адрес шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Установите этот флажок, чтобы при подключении приложения, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей, если Сервер администрирования недоступен. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию флажок снят.

- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию параметр включен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

  Если этот параметр включен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

Если этот параметр выключен, Агент администрирования подключается к Серверу, используя исходные параметры, указанные при установке.

Параметр доступен, если параметр **Использовать только для получения обновлений** выключен.

По умолчанию параметр выключен.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

Политики и профили политик

В OSMP Console можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky EDR Expert предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей политик.

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (🔒). В таблице ниже показаны состояния значка замка:

Статусы значка замка

Состояние	Описание
Undefined	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.
Enforce	Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

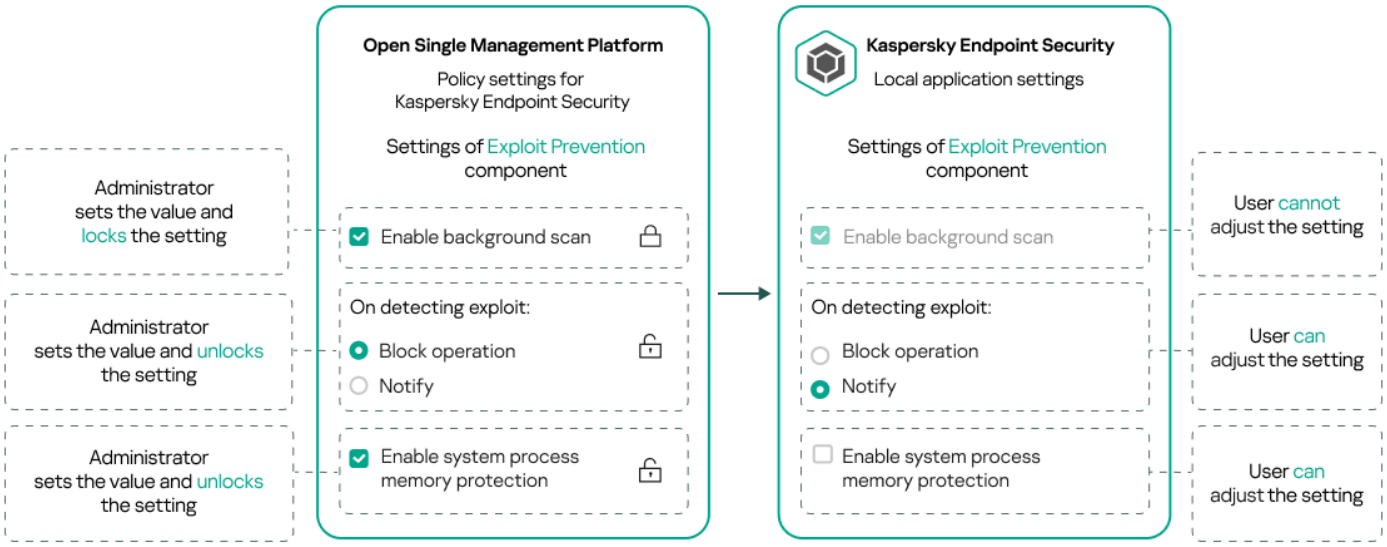
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



Замки и параметры приложения "Лаборатории Касперского"

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

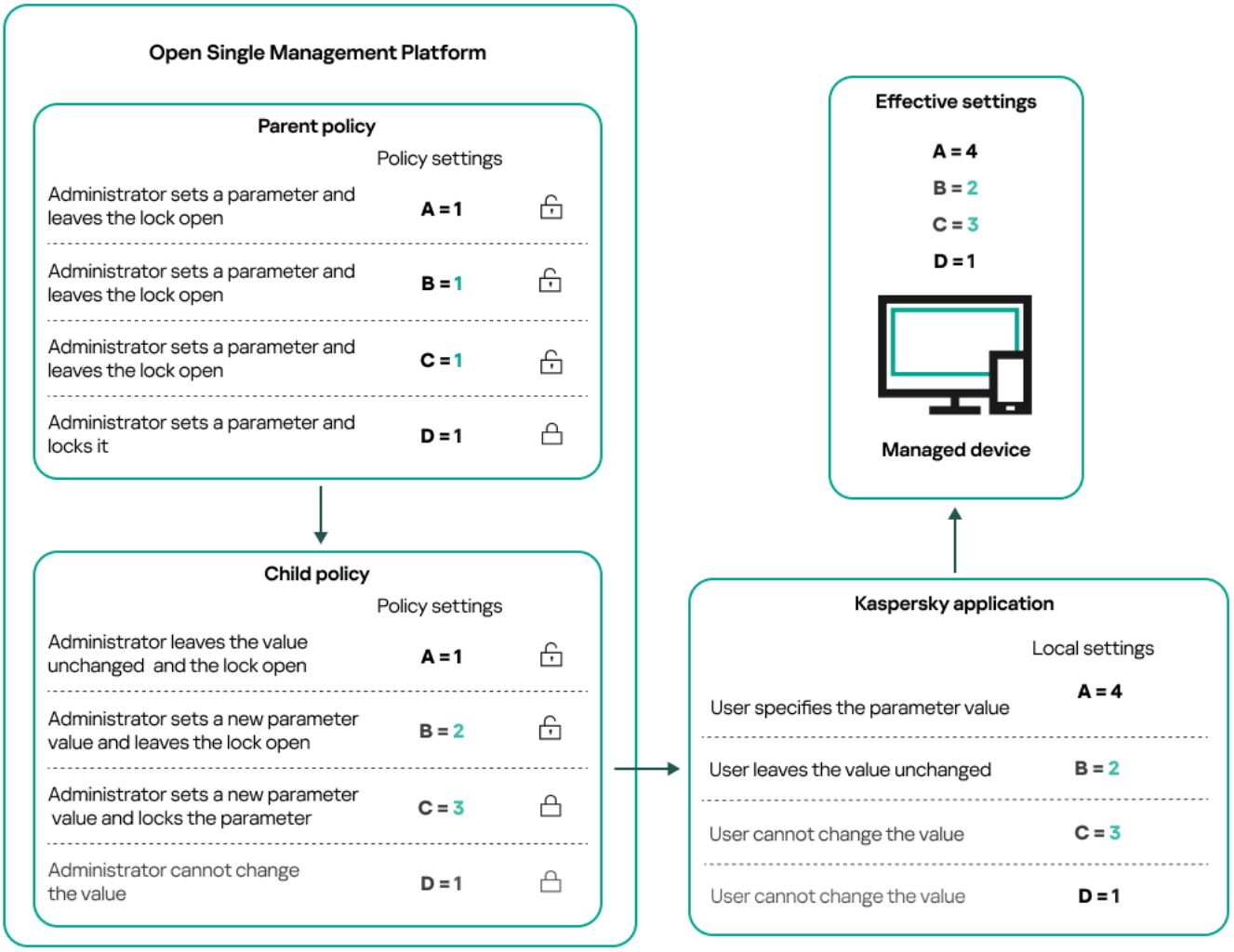
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования. Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).

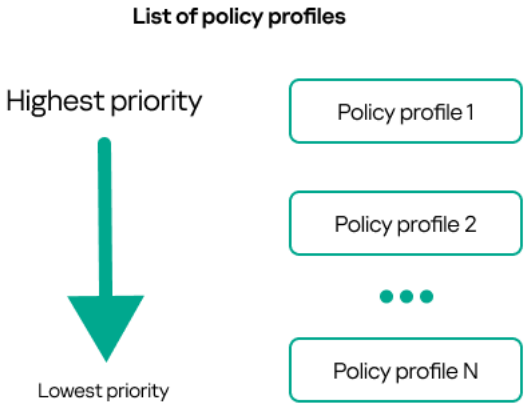


Иерархия политик

Профили политик в иерархии политик

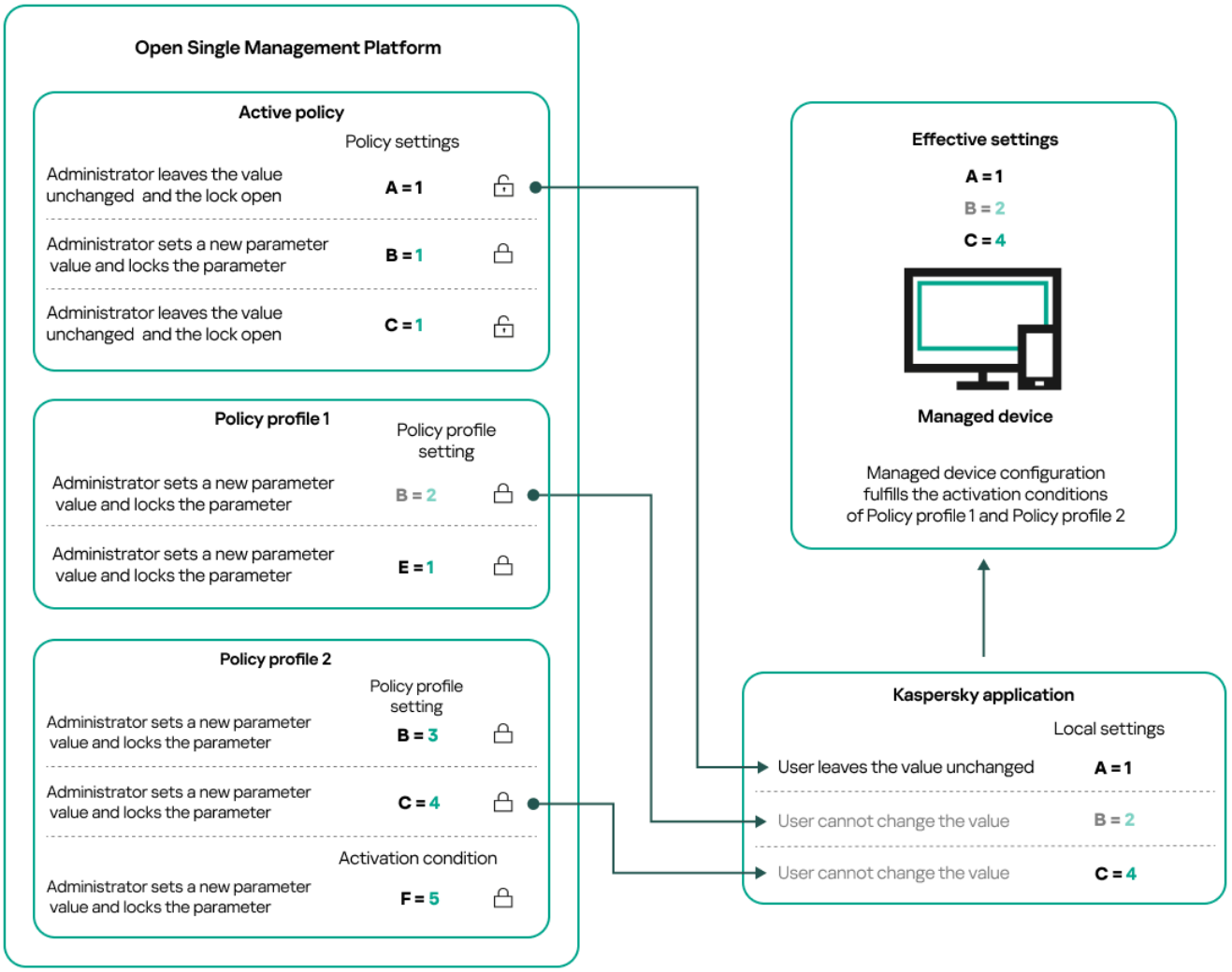
Профили политики имеют следующие условия назначения приоритета:

- Положение профиля в списке профилей политики обозначает его приоритет. Вы можете изменить приоритет профиля политики. Самая высокая позиция в списке обозначает самый высокий приоритет (см. рисунок ниже).



Определение приоритета профиля политики

- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).



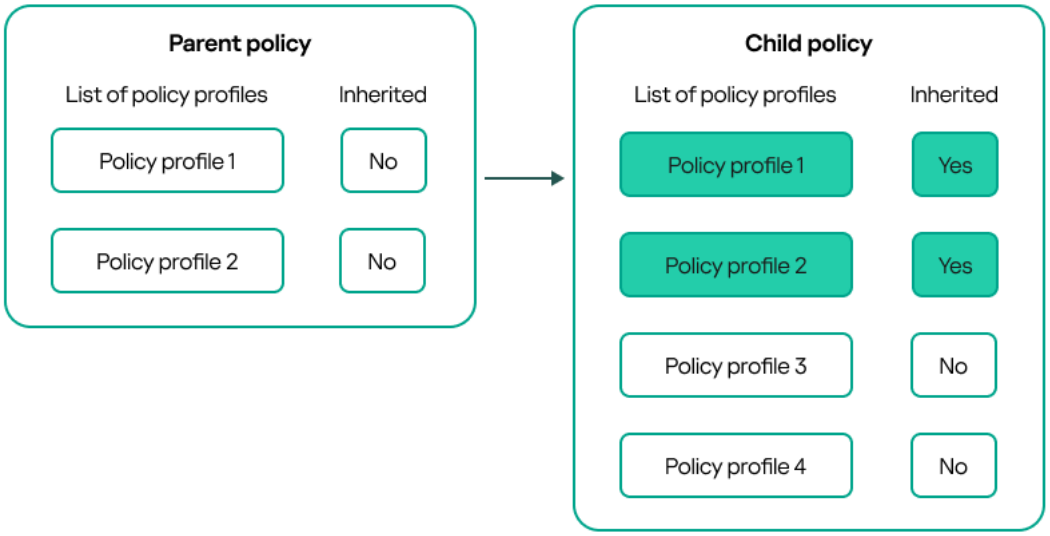
Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.

- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).



Наследование параметров профилей политики

Профили политики с одинаковыми именами

Если на разных уровнях иерархии есть две политики с одинаковыми именами, эти политики работают в соответствии со следующими правилами:

- Заблокированные параметры и условие активации профиля для профиля политики более высокого уровня изменяют параметры и условие активации профиля для профиля политики более низкого уровня (см. рисунок ниже).

Дочерний профиль наследует значения параметров из родительского профиля политики

- Разблокированные параметры и условие активации профиля для профиля политики более высокого уровня не изменяют параметры и условие активации профиля для профиля политики более низкого уровня.

Как параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

Управление политиками

В этом разделе описывается управление политиками и предоставляется информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

Чтобы просмотреть список политик:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

Чтобы создать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите группу администрирования, для которой нужно создать политику:

   - Для корневой группы.

     В этом случае вы можете перейти к следующему шагу.

   - Для подгруппы:

     a. Нажмите на кнопку **Показать иерархию** в верхней части страницы.

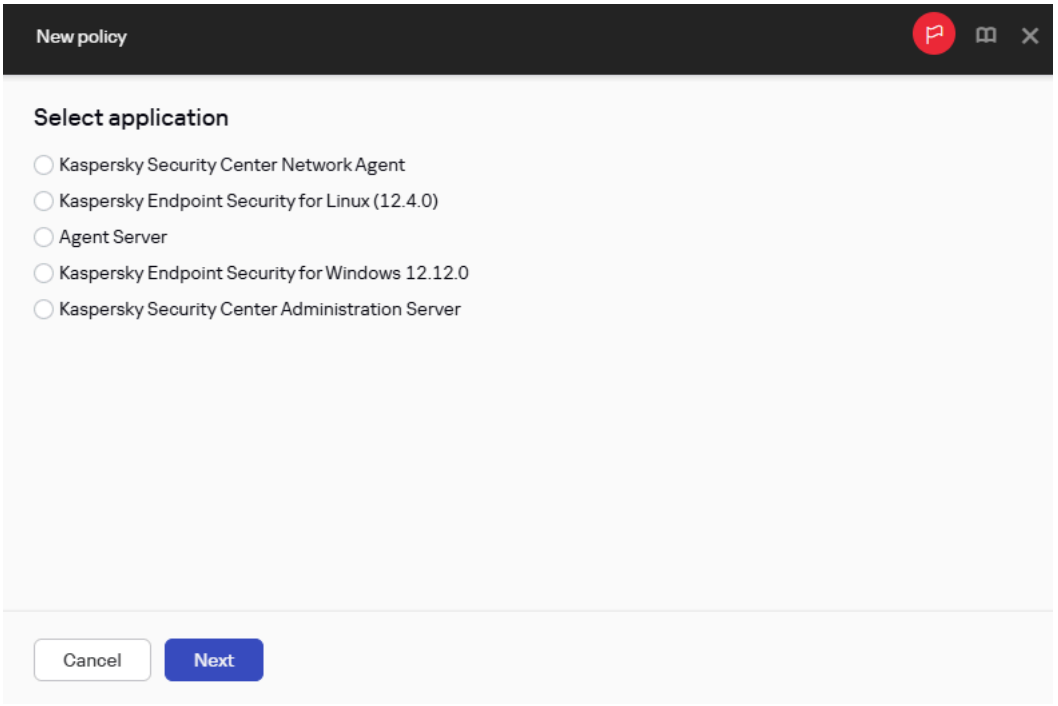
     b. Название кнопки изменится на **Скрыть иерархию**.

     c. В открывшемся окне нажмите на название нужной подгруппы.

   Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

3. Нажмите на кнопку **Добавить**.

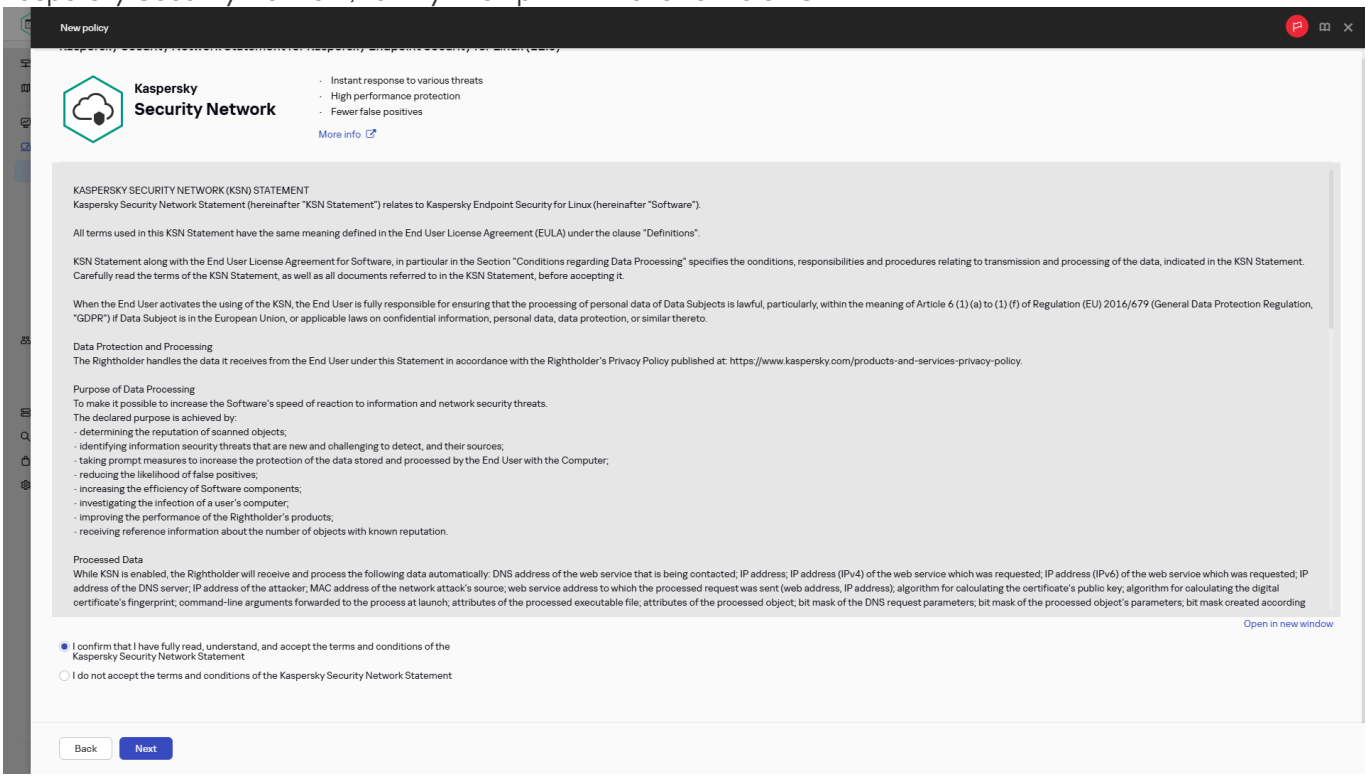
Откроется окно **Выберите приложение**.



Создание политики

4. Выберите приложение, для которого требуется создать политику.

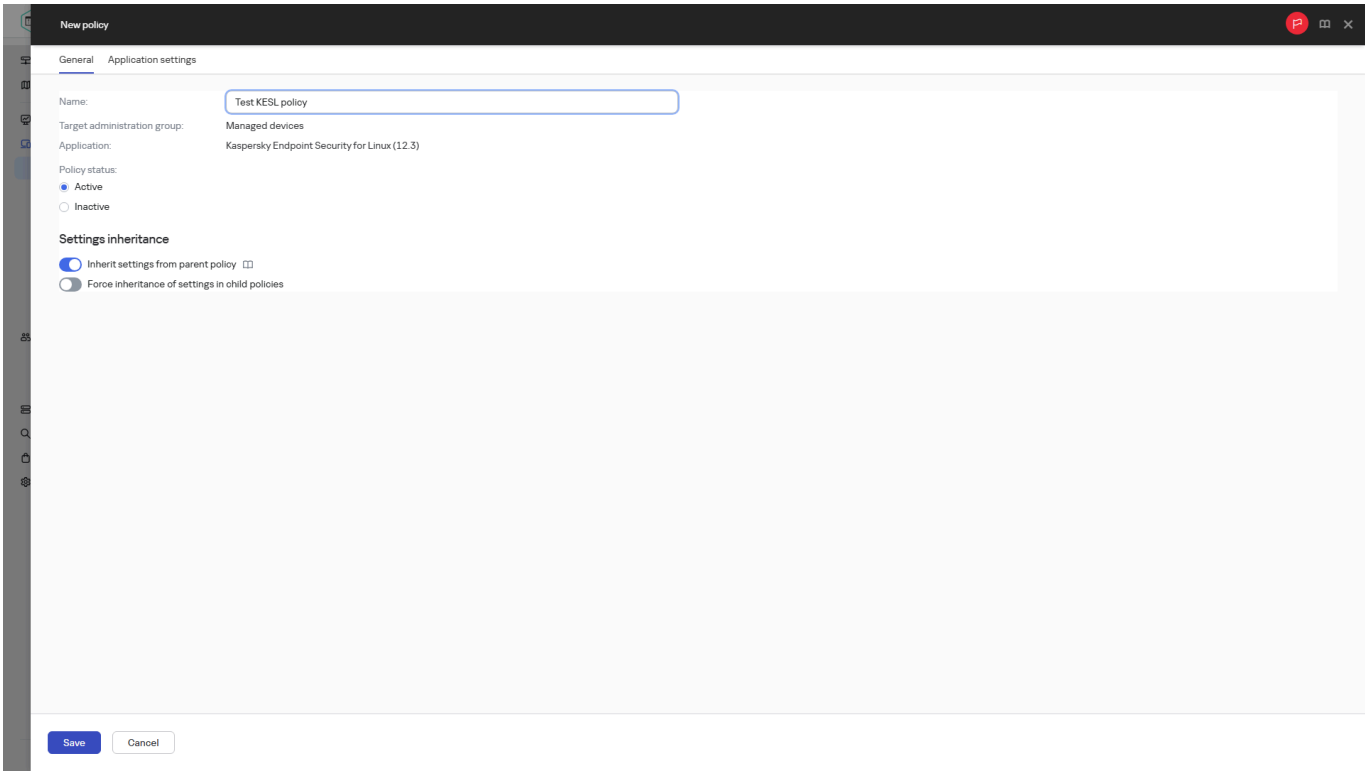
5. Если Kaspersky Security Network поддерживается приложением "Лаборатории Касперского", для которого вы создаете политику, вам будет предложено подтвердить Положение о KSN. Если вы хотите использовать Kaspersky Security Network, вам нужно принять Положение о KSN.



Принятие Положения о KSN

6. Нажмите на кнопку **Далее**.

Откроется окно параметров новой политики на вкладке **Общие**. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.



Окно параметров новой политики

7. Выберите вкладку **Параметры приложения**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.

8. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Справка Kaspersky Endpoint Security for Linux
   - Справка Kaspersky Endpoint Security for Windows

   Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.

   Отображается уведомление со следующим сообщением: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

   Если политика проходит проверку, отображается следующее уведомление: **Политика сохранена**.

Если политика не проходит проверку, отображается следующее уведомление: **Не удалось сохранить и распространить политику через иерархию Серверов администрирования. Обратитесь в Службу технической поддержки**. Вы можете проверить и изменить параметры политики, а затем повторить попытку. Если устранить проблему не удается, обратитесь в Службу технической поддержки.

В результате добавленная политика отображается в списке политик. После создания политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

Общие параметры политик

Общие

На вкладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

  Активна

  Если выбран этот вариант, политика становится активной.

  По умолчанию выбран этот вариант.

  Для автономных пользователей

  Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

  Неактивна

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  Наследовать параметры родительской политики

  Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

  По умолчанию параметр включен.

  Обеспечить принудительное наследование параметров для дочерних политик

  Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

  - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
  - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

  Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

  По умолчанию параметр выключен.

Настройка событий

На вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Критическое**

  Раздел **Критическое** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

  Вы можете указать количество дней хранения событий и выбрать, где хранить события:

  - **Экспортировать в SIEM-систему по протоколу syslog**
  - **Хранить в журнале событий ОС на устройстве**
  - **Хранить в журнале событий ОС на Сервере администрирования**

- **Уведомления о событиях**

  Вы можете выбрать способ уведомления о событии:

  - **Уведомлять по электронной почте**
  - **Уведомлять по SMS**
  - **Уведомлять запуском исполняемого файла или скрипта**
  - **Уведомлять по SNMP**

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

На вкладке **Настройка событий** отображаются уведомления при добавлении новых типов событий (например, в новой версии приложения), а также можно применить новые параметры, нажав на кнопку **Сохранить** или **Сохранить и закрыть**.

История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики, сравнить ревизии политики, и при необходимости откатить изменения политики.

Изменение политики

Чтобы изменить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.

3. Укажите общие параметры и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Документация Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

4. Нажмите на кнопку **Сохранить**.

   Отображается уведомление со следующим сообщением: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

   Если политика проходит проверку, отображается следующее уведомление: **Политика сохранена**.

   Если политика не проходит проверку, отображается следующее уведомление: **Не удалось сохранить и распространить политику через иерархию Серверов администрирования. Обратитесь в Службу технической поддержки**. Вы можете проверить и изменить параметры политики, а затем повторить попытку. Если устранить проблему не удается, обратитесь в Службу технической поддержки.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**. После изменения политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

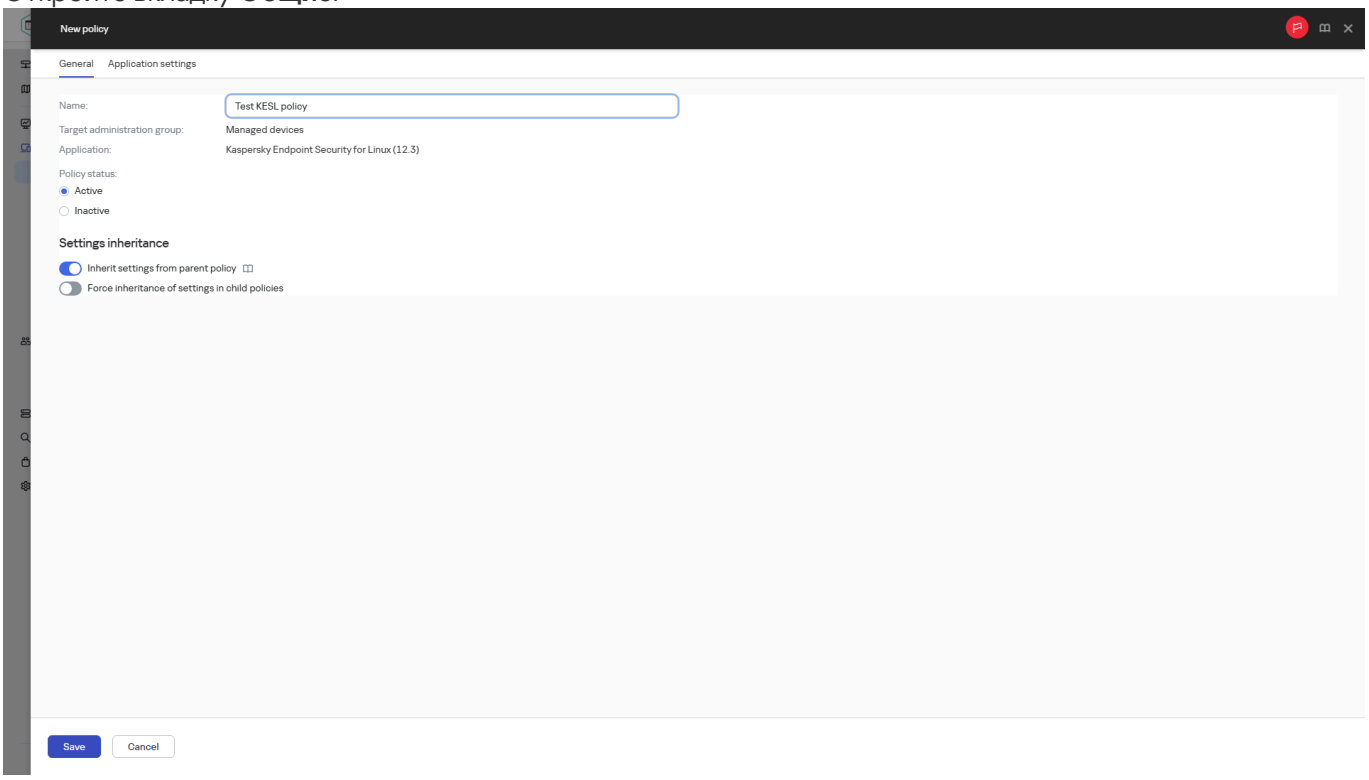
При необходимости вы можете сравнить ревизии политики. Параметр доступен для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Включение и выключение параметра наследования политики

Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.

2. Откройте вкладку **Общие**.



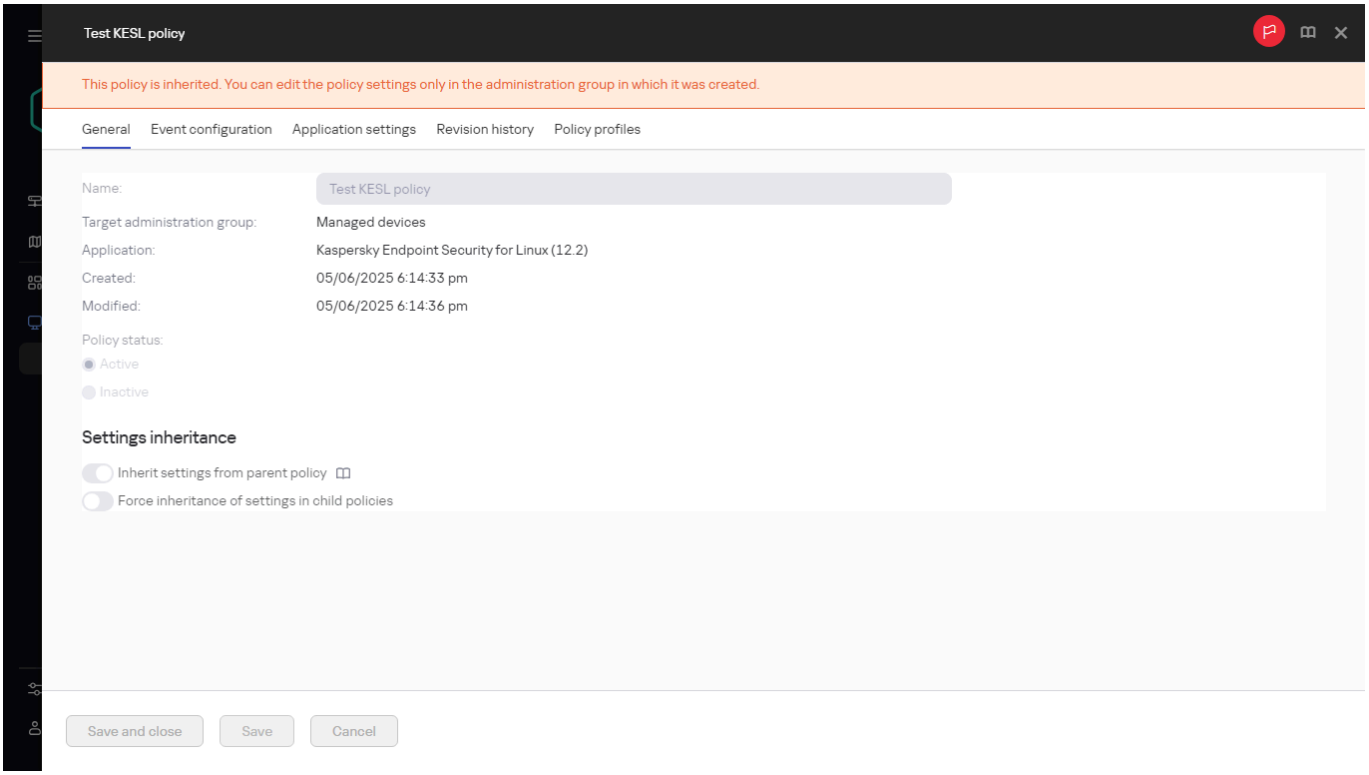
Создание политики

3. Включение или выключение наследования политики:

- Если вы включили параметр **Наследовать параметры родительской политики** для дочерней группы и администратор заблокировал некоторые параметры в родительской политике, то вы не можете изменить эти параметры политики для дочерней политики.

- Если вы выключили параметр **Наследовать параметры родительской политики** для дочерней политики, то вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.

- Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.



Заблокированные параметры политик

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или нажмите на кнопку **Отмена**, чтобы отклонить изменения.

По умолчанию, параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

Чтобы скопировать политику в другую группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок напротив политики (или политик), которую требуется скопировать.

3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.

4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).

5. Нажмите на кнопку **Копировать** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

> При перемещении политики в другую группу администрирования история изменений политики удаляется. На вкладке **История ревизий** отображается информация только о последних изменениях.

Чтобы переместить политику в другую группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок напротив политики (или политик), которую требуется переместить.

3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.

4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).

5. Нажмите на кнопку **Переместить** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

   Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

   Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Экспорт политики

Open Single Management Platform позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

   Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

Импорт политики

Open Single Management Platform позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику, ее параметры и профили политики.

Чтобы импортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.
5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.
6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

> Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Принудительная синхронизация

Несмотря на то, что Kaspersky EDR Expert автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору требуется точно знать, была ли выполнена синхронизация для определенного устройства в данный момент.

Синхронизация одного устройства

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать сейчас**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:
   - Запустите выборку устройств, чтобы просмотреть список устройств.
   - В главном окне приложения перейдите в разделе **Управление активами** → **Активы (Устройства)** и выберите группу администрирования, содержащую устройства для синхронизации:
     - Для корневой группы вы можете перейти к следующему шагу.
     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне нажмите на имя подгруппы.

       Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.

3. Над списком управляемых устройств нажмите на кнопку с многоточием (...), а затем нажмите на кнопку **Синхронизировать сейчас**.

   Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.

4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.

3. Перейдите на вкладку **Приложения**.

4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

   Откроется окно политики приложения, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

Просмотр диаграммы состояния применения политики

В Open Single Management Platform вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.

3. В появившемся меню выберите ссылку **Результаты применения**.

Откроется окно **Результат распространения <название политики>**.

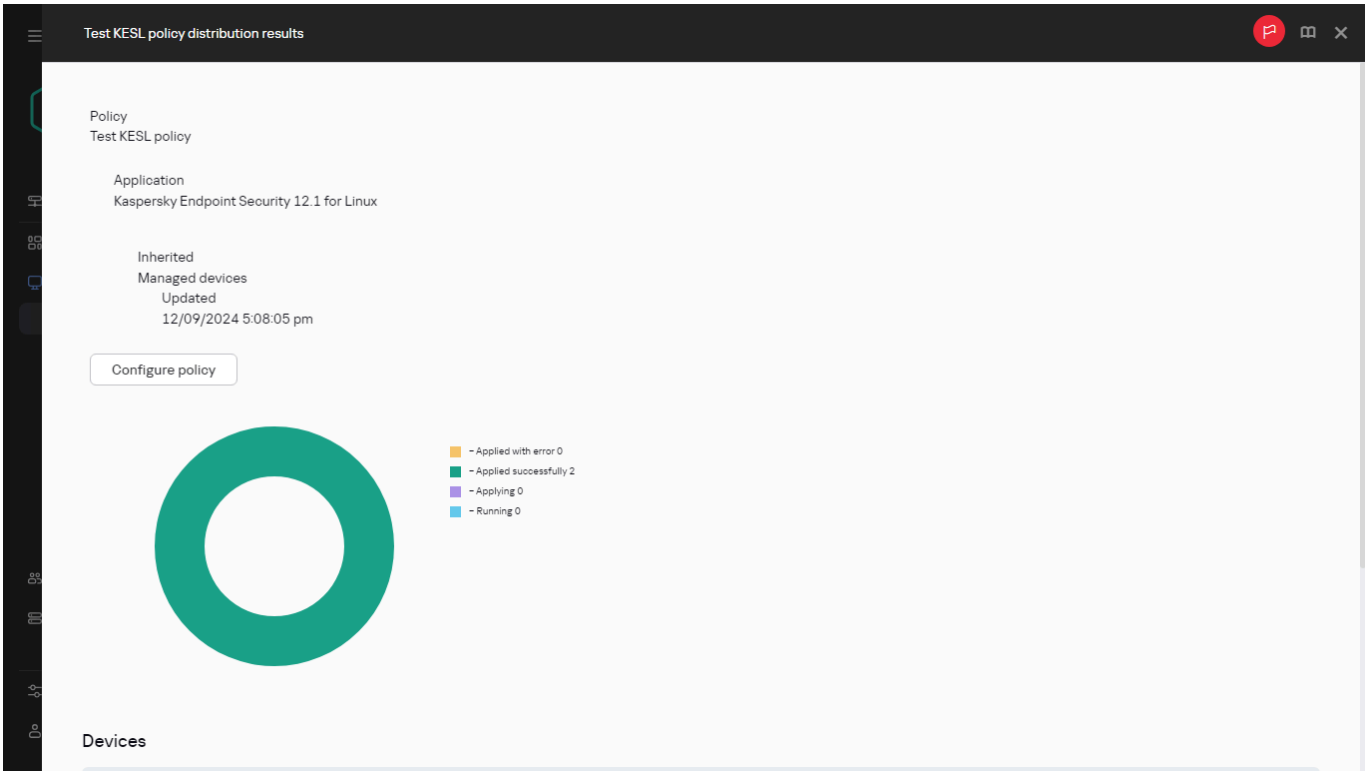


Диаграмма состояния применения политики

4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В главном окне приложения перейдите в раздел **Параметры** → **Параметры интерфейса**.

2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.

3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Автоматическая активация политики по событию "Вирусная атака"

Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите раздел **Вирусная атака**.

3. В правой панели нажмите на ссылку **Настроить активацию политик по возникновению события "Вирусная атака"**.

   Откроется окно **Активация политик**.

4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам запись и затем нажмите на кнопку **Добавить**.

   Откроется окно с группой администрирования **Управляемые устройства**.

5. Нажмите на значок шеврона (>) рядом с **Управляемые устройства**.

   Отобразится иерархия групп администрирования и их политик.

6. В иерархии групп администрирования и их политик нажмите на название политики (или политик), которая активируется при возникновении вирусной атаки.

   Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.

7. Нажмите на кнопку **Сохранить**.

   Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок рядом с именем политики, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.

3. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Политика и все ее профили политики удалены. После удаления политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, копировании профиля политики, создании правила активации профиля политики, удалении, экспорте и импорте профиля политики.

Просмотр профилей политики

Чтобы просмотреть профили политики:

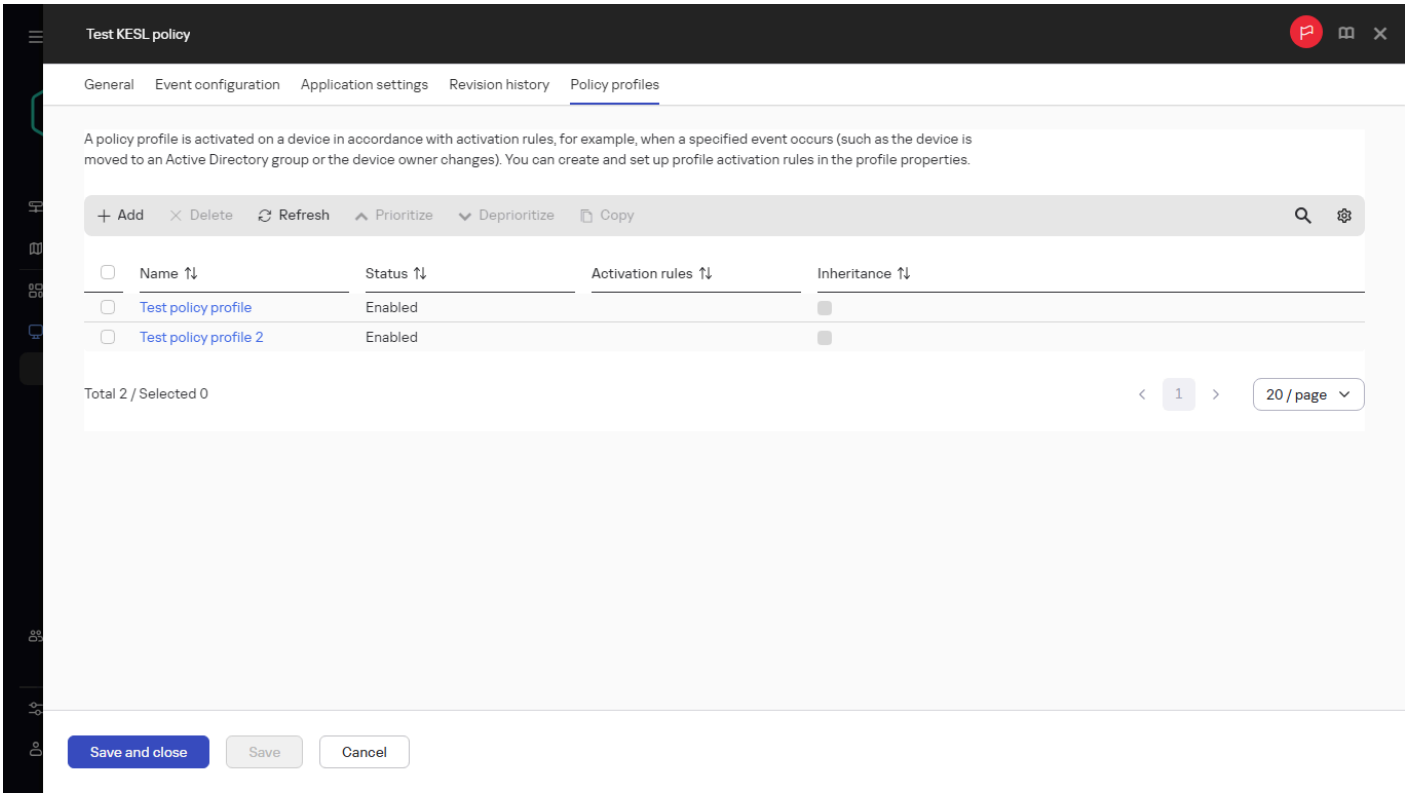
1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.

3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.



Список профилей политики

Изменение приоритета профиля политики

Чтобы изменить приоритет профиля политики:

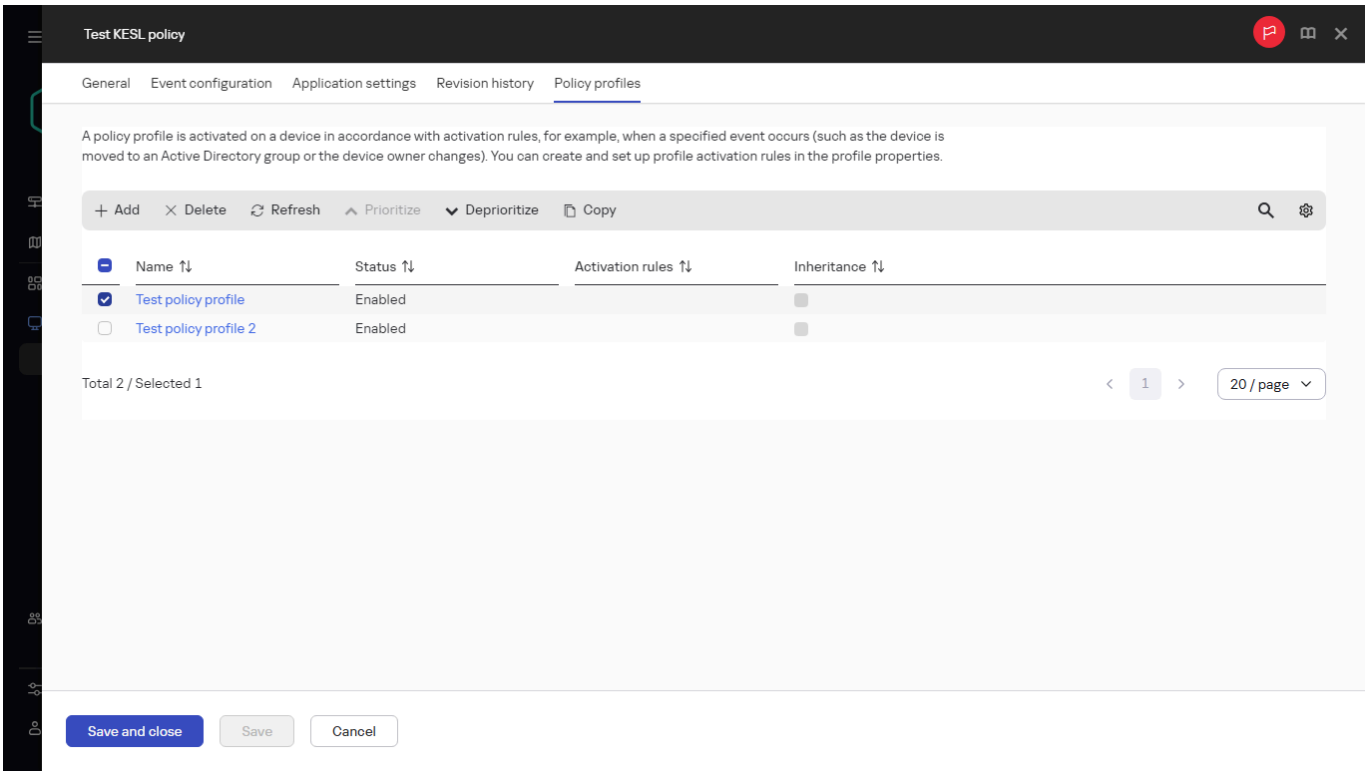
1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.

3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

   Чем выше расположен профиль политики в списке, тем выше его приоритет.



4. Нажмите на кнопку **Сохранить**.

   Приоритет выбранного профиля политики изменен и применен.

Создание профиля политики

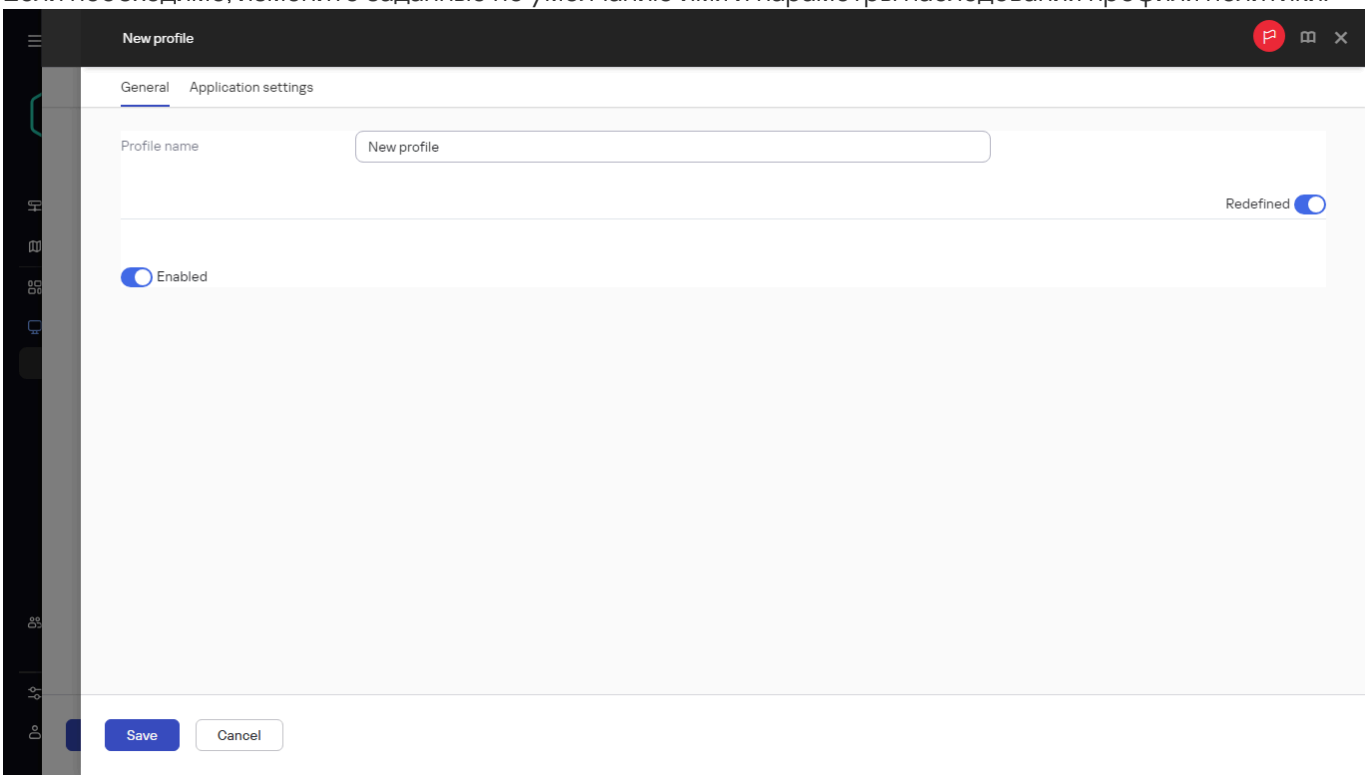
Чтобы создать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. Нажмите на кнопку **Добавить**.

3. Если необходимо, измените заданные по умолчанию имя и параметры наследования профиля политики.



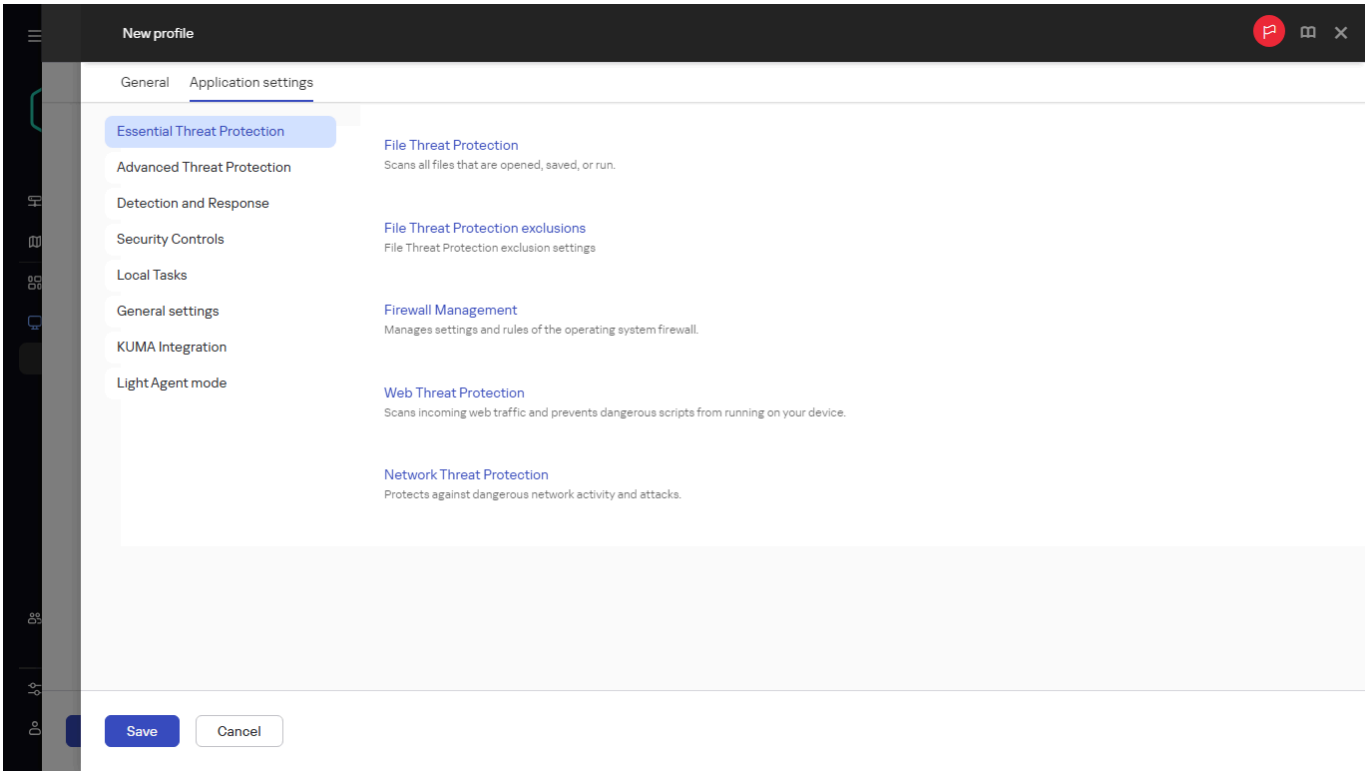
Создание профиля политики

4. Выберите вкладку **Параметры приложения**.

   Можно также нажать на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.

5. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.



Указание параметров профиля политики

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля.

   Профиль политики отобразится в списке профилей политики.

Копирование профиля политики

Вы можете скопировать профиль политики в текущую политику или в другую политику, например, если вы хотите иметь идентичные профили политик для разных политик. Вы также можете использовать копирование, если хотите иметь два или более профилей политики, которые отличаются небольшим количеством параметров.

Чтобы скопировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На вкладке **Профили политики** выберите профиль, который требуется скопировать.

3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне выберите политику, в которую требуется скопировать профиль политики.

   Вы можете скопировать профиль политики в эту же политику или в политику, которую вы выбрали.

5. Нажмите на кнопку **Копировать**.

Профиль политики скопирован в политику, которую вы выбрали. Новый скопированный профиль политики имеет самый низкий приоритет. Если вы скопировали профиль политики в эту же политику, к имени такого профиля добавляется окончание вида (<порядковый номер>), например: (1), (2).

Позже вы можете изменить параметры профиля политики, включая его имя и приоритет. В этом случае исходный профиль политики не будет изменен.

Создание правила активации профиля политики

Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики.

3. На вкладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   Общие правила активации профиля политики

   Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

   Для этого параметра на следующем шаге укажите:

   Статус устройства

   Определяет условие присутствия устройства в сети:

   - **В сети** – устройство находится в сети, Сервер администрирования доступен.
   - **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
   - **Неизвестно** – критерий не применяется.

   Параметры сетевого местоположения устройства

   Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

   Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

   Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

   - **Правила для выбранного владельца устройства**

     Для этого параметра на следующем шаге укажите:

     Владелец устройства

Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

Владелец устройства включен во внутреннюю группу безопасности

Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky EDR Expert. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky EDR Expert. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации профиля политики на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  Объем оперативной памяти (МБ)

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - объем оперативной памяти устройства меньше указанного значения (знак "<");
  - объем оперативной памяти устройства больше указанного значения (знак ">").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Количество логических процессоров

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - количество логических процессоров устройства меньше или равно указанному значению (знак " <");
  - количество логических процессоров устройства больше или равно указанному значению (знак ">").

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

  Активировать профиль политики по наличию роли у владельца устройства

  Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

  Для этого параметра на следующем шаге укажите:

  Список тегов

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

  Применить к устройствам без выбранных тегов

  Включите параметр, если необходимо инвертировать выбор тегов.

  Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

- **Правила для использования Active Directory**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

  Для этого параметра на следующем шаге укажите:

  Членство владельца устройства в группе безопасности Active Directory

  Если параметр включен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Членство устройства в группе безопасности Active Directory

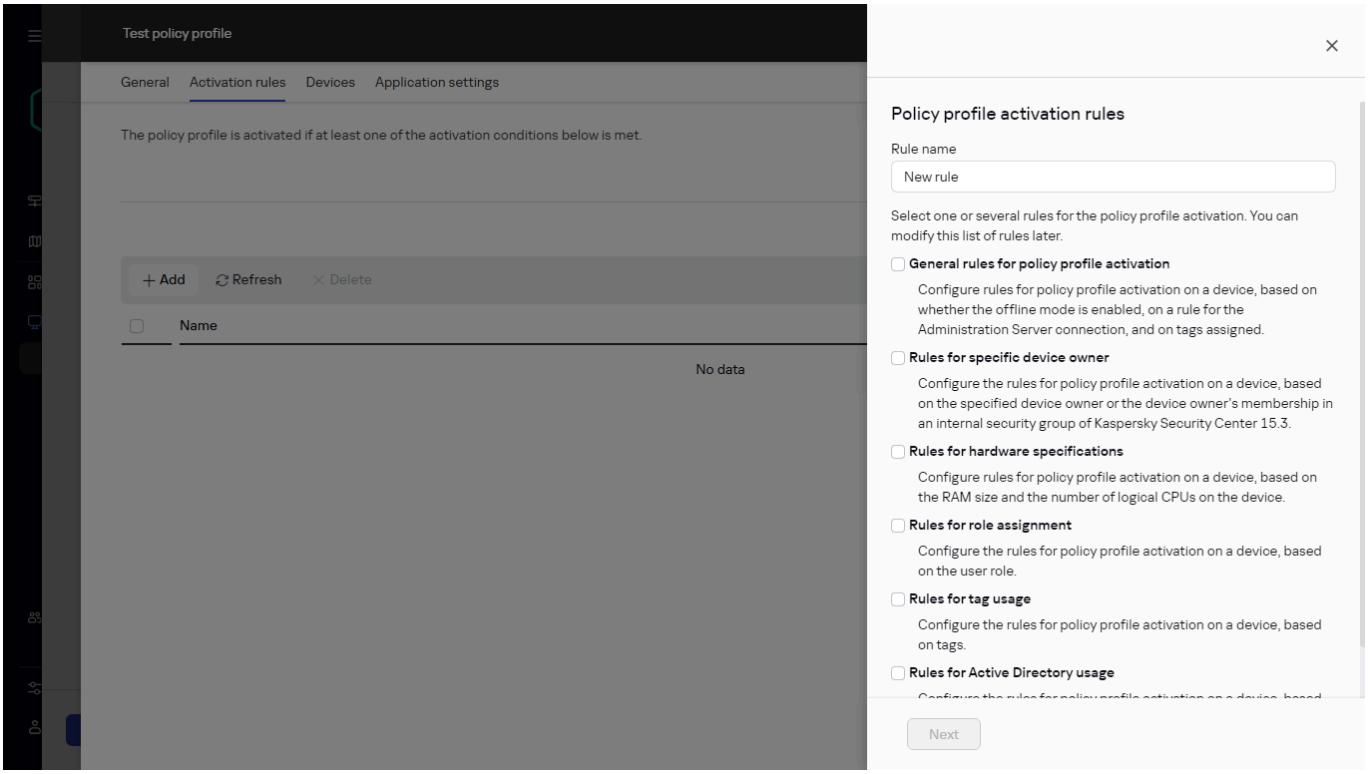
  Если параметр включен, профиль политики активируется на устройстве. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Размещение устройства в подразделении Active Directory

Если параметр включен, профиль политики активируется на устройстве, которое входит в указанное подразделение Active Directory (OU). Если параметр выключен, критерий активации профиля не применяется.

По умолчанию параметр выключен.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.



Создание правила активации профиля политики.

6. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

   В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики на вкладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых приложений, установленных на устройствах групп нижнего уровня.

Экспорт и импорт профиля политики

Вы можете сохранить профиль политики в файл KLPROF без экспорта политики, а затем использовать этот файл KLPROF для импорта сохраненного профиля в политику.

Это позволяет быстро восстановить параметры профиля политики вместо их повторной настройки.

Профиль политики импортируется в политику той же версии приложения, из которой вы экспортировали профиль. Для приложений, поддерживающих обратную совместимость политик (например, Kaspersky Endpoint Security for Windows), вы можете импортировать профили политики в разные версии политики.

Чтобы экспортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите экспортировать.

3. В панели инструментов нажмите на кнопку **Экспортировать**.

4. В открывшемся окне укажите директорию, в которую вы хотите сохранить в файл с профилем политики.

   При необходимости измените имя файла.

5. Нажмите на кнопку **Сохранить**.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Чтобы импортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. В панели инструментов нажмите на кнопку **Импортировать**.

3. В открывшемся окне выберите файл KLPROF с нужным профилем политики и нажмите на кнопку **Открыть**.

   Максимальный размер импортируемого файла – 4 МБ.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Профиль политики импортируется с именем, которое он имел при экспорте, а не с именем файла KLPROF.
Файл импортируется со статусом **Выключен** и самым низким приоритетом, независимо от приоритета, который был у профиля политики перед экспортом.

Вы не можете выполнить импорт в следующих случаях:

- У политики уже есть профиль с таким же именем.
- Количество профилей в политике равно 100.

Параметры политики Агента администрирования

Чтобы настроить параметры политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования. Окно свойств содержит вкладки и параметры, описанные ниже.

См. таблицу сравнения, в которой подробно описано применение параметров, описанных ниже, в зависимости от используемой операционной системы.

Общие

На этой вкладке можно изменить название политики, состояние политики и настроить наследование параметров политики:

- В поле **Имя** вы можете изменить название политики.
- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

  Активна

  Если выбран этот вариант, политика становится активной.

  По умолчанию выбран этот вариант.

  Неактивна

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  Наследовать параметры родительской политики

  Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

  По умолчанию параметр включен.

  Обеспечить принудительное наследование параметров для дочерних политик

  Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

  - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
  - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

  Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

  По умолчанию параметр выключен.

Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределяются по уровням важности в следующих разделах:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и срок хранения событий на Сервере администрирования по умолчанию (в днях). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки приложений и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

> Если Агент администрирования обнаруживает проблему безопасности, вы можете управлять этой проблемой безопасности с помощью параметров управляемого устройства.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

Распространять файлы только через точки распространения

Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования.

> Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Open Single Management Platform установлен в качестве источника обновлений в задачах обновления.

По умолчанию параметр выключен.

Максимальный размер очереди событий (МБ)

В поле можно указать максимальное место на диске, которое может занимать очередь событий.

По умолчанию указано значение 2 МБ.

Приложение может получать расширенные данные политики на устройстве

Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security for Linux). Передаваемая информация отображается в интерфейсе приложения безопасности.

Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики в момент доставки политики на управляемое устройство;
- название политики для автономных пользователей в момент доставки политики на управляемое устройство (недоступно для Агента администрирования для Linux);
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политик с указанием их названий и приоритетов на момент доставки политики на управляемое устройство.

Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы

Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

Использовать пароль деинсталляции

Если параметр включен, при нажатии на кнопку **Изменить** можно указать пароль для утилиты klmover.

По умолчанию параметр выключен.

Выключите этот параметр, чтобы удалить Агент администрирования удаленно.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования:

Информация об установленных приложениях

Если этот параметр включен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

По умолчанию параметр включен.

Включить информацию о патчах

Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

По умолчанию параметр включен. Доступен только для Windows.

Информация об обновлениях Центра обновления Windows

Если параметр установлен, на Сервер администрирования отправляется информация об обязательных обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

По умолчанию параметр включен. Доступен только для Windows.

Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

Информация об уязвимостях в приложениях и соответствующих обновлениях

Если этот параметр включен, информация об уязвимостях в приложениях сторонних производителей (включая программное обеспечение Microsoft), обнаруженных на управляемых устройствах, и об обновлениях программного обеспечения для закрытия уязвимостей (не включая программное обеспечение Microsoft) отправляется на Сервер администрирования.

Выбор этого параметра (**Информация об уязвимостях в приложениях и соответствующих обновлениях**) увеличивает нагрузку на сеть, загрузку диска Сервера администрирования и потребление ресурсов Агентом администрирования.

По умолчанию параметр включен. Доступен только для Windows.

Для управления обновлениями приложений Microsoft используйте параметр **Информация об обновлениях Центра обновления Windows**.

Информация о реестре оборудования

Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** вы можете включить проверку исполняемых файлов на наличие уязвимостей:

Проверять исполняемые файлы на наличие уязвимостей при запуске

Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию параметр включен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если во время работы, установки или удаления приложения требуется перезагрузить операционную систему управляемого устройства:

Не перезагружать операционную систему

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

При необходимости перезагрузить операционную систему автоматически

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

Запрашивать у пользователя

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

Повторять запрос периодически через (мин)

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

Принудительно перезагружать через (мин)

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

Принудительно закрывать приложения в заблокированных сеансах

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Управление патчами и обновлениями

В разделе Управление патчами и обновлениями можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"

Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

По умолчанию параметр включен.

Скачивать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)

Если параметр включен, офлайн-модель получения обновлений используется. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

По умолчанию параметр включен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключиться к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:

  Период синхронизации (мин)

  Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал) равным 15 минут на 10 000 управляемых устройств.

  Сжимать сетевой трафик

  Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

  > Нагрузка на центральный процессор клиентского компьютера может возрасти.

  По умолчанию флажок установлен.

  Открывать порты Агента администрирования в брандмауэре Microsoft Windows

Если параметр включен, порты, необходимые для работы Агента администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

По умолчанию параметр включен.

Использовать SSL-соединение

Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию параметр включен.

Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию

Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

По умолчанию параметр включен.

- **Использовать UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

  Выберите этот параметр, если вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В подразделе **Профили соединений** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен:

Параметры сетевого местоположения

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

Профили подключения к Серверу администрирования

Вы можете просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

Включить автономный режим, когда Сервер администрирования недоступен

Если параметр включен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

Если параметр выключен, приложения будут использовать активные политики.

По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

Подключаться при необходимости

Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

По умолчанию выбран этот вариант.

Подключаться в указанные периоды

Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

Сеть Windows

Параметр доступен только для точек распространения с операционной системой Windows.

Если этот параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

Период обнаружения устройств для Агента администрирования можно настроить в полях **Период опроса Windows-доменов (мин)** (для быстрого опроса сети Windows) и **Период опроса сети (мин)** (для полного опроса сети Windows).

По умолчанию параметр выключен.

IP-диапазоны

Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

Если параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

По умолчанию параметр выключен.

Zeroconf

Если этот параметр включен, точка распространения автоматически опрашивает сеть с устройствами IPv6, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае включенный опрос IP-диапазонов игнорируется, так как точка распространения опрашивает всю сеть.

Чтобы можно было начать использовать Zeroconf, должны быть выполнены следующие условия:

- Точка распространения должна работать под управлением Linux.
- Вам нужно установить утилиту avahi-browse на точку распространения.

Если этот параметр отключен, точка распространения не опрашивает сети с устройствами IPv6.

По умолчанию параметр выключен.

Контроллеры доменов

Если этот параметр включен, точка распространения автоматически выполняет опрос контроллеров домена в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

Если параметр выключен, точка распространения не выполняет опрос контроллеров домена.

Периодичность опроса контроллеров домена для версий Агента администрирования ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

По умолчанию параметр выключен.

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать параметры доступа к интернету:

- **Использовать прокси-сервер**

  Если этот параметр включен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете.

- **Адрес**

- **Номер порта**

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки Kaspersky Security Network (KSN) запросов от управляемых устройств:

Включить прокси-сервер KSN на стороне точки распространения

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

Пересылать KSN запрос Серверу администрирования

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

Доступ к облачной службе KSN/KPSN непосредственно через интернет

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

TCP-порт

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

UDP-порт

Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

HTTPS-порт

Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **HTTPS-порт**. По умолчанию параметр выключен. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

Обновления (точки распространения)

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского".

Управление учетными записями (только для Linux)

Раздел **Управление учетными записями (только для Linux)** состоит из трех подразделов:

- **Управление пользовательскими сертификатами**
- **Добавление или изменение групп локальных администраторов**
- **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений**

В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

Установить корневые сертификаты

Если этот параметр включен, сертификаты, добавленные в таблицу, будут установлены на указанных устройствах.

Если этот параметр выключен, сертификаты не будут установлены на указанные устройства.

По умолчанию параметр выключен.

Добавить

Нажав на эту кнопку открывается окно, в котором можно добавить сертификат.

Размер сертификата должен быть меньше 10 МБ.

Kaspersky Security Center поддерживает сертификаты с расширениями CER, CRT, CERT, PEM и KEY.

В подразделе **Добавление или изменение групп локальных администраторов** вы можете управлять группами локальных администраторов. Эти группы используются, например, при отзыве прав локального администратора. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

Добавить

Нажмите на эту кнопку, чтобы добавить локальную группу администраторов.

Изменить

Нажмите на эту кнопку, чтобы изменить локальную группу администраторов.

Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

Удалить

Нажмите на эту кнопку, чтобы удалить выбранную группу локальных администраторов из таблицы.

Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

В подразделе **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений** вы можете настроить управление файлом sudoers. Привилегированные группы и пользователи устройства определяются файлом sudoers на устройстве. Файл sudoers находится в папке `/etc/sudoers`. Вы можете загрузить референсный файл sudoers, чтобы защитить файл sudoers от изменений. Это предотвратит нежелательные изменения файла sudoers.

Недопустимый референсный файл sudoers может привести к неисправности устройства пользователя.

Контролировать файл sudoers

Если этот параметр включен, файл sudoers будет заменен текущим референсным файлом sudoers.

Если этот параметр выключен, файл sudoers остается без изменений.

По умолчанию параметр выключен.

Референсный файл sudoers

В этом поле отображается название загруженного референсного файла sudoers.

Загрузить

Нажмите на эту кнопку, чтобы загрузить референсный файл sudoers.

Текущий референсный файл sudoers

Нажмите на эту кнопку, чтобы просмотреть текущий файл sudoers.

История ревизий

На вкладке **История ревизий** вы можете:

- Просмотреть и сохранить историю изменений политики.
- Откатить к ревизии политики.
- Добавить и изменить описание ревизии политики.
- Сравнить ревизии политики.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, Linux и macOS.

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Установка Агента администрирования в тихом режиме	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓	✓
Автоматическая установка обновлений и патчей для компонентов Kaspersky EDR Expert	✓	✓	—
Автоматическое распространение ключа	✓	✓	✓
Принудительная синхронизация	✓	✓	✓ За исключением push-сервера
Точка распространения			
Использование точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Расчет количества и конфигурации точек распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Без использования Network Location Awareness (NLA).	✓ Без использования Network Location Awareness (NLA).
Офлайн-модель получения обновлений	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Опрос сети	✓ • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory) Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Опрос IP-диапазонов Опрос Zeroconf Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—

Функция Агента администрирования	Windows	Linux	macOS
Запуск службы прокси-сервер KSN на стороне точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	—
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	— Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Использовать в качестве push-сервера	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	—
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	✓	✓ Подробнее см. в статье Удаленная установка приложений на устройства с операционной системой macOS.
Настройка обновлений операционной системы в политике Агента администрирования	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Просмотр информации об уязвимостях в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Поиск уязвимостей в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Обновления программного обеспечения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Оптимизация параметров для VDI	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Поддержка динамических виртуальных машин	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Мониторинг состояния антивирусной защиты	✓	✓	✓
Управление перезагрузкой устройств	✓	—	—
Поддержка отката файловой системы	✓	✓	✓
Использование Агента администрирования в качестве шлюза соединений	✓	✓	✓
Менеджер соединений	✓	✓	✓
Профили соединения для автономных пользователей	✓	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению)	✓	✓	✓
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	✓	✓ С помощью системы Virtual Network Computing (VNC).

Функция Агента администрирования	Windows	Linux	macOS
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓
Просмотр информации об аппаратном обеспечении клиентских устройств	✓	✓ Информация об аппаратном обеспечении устройств с операционной системой Linux передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства.	✓ Информация об аппаратном обеспечении устройств с операционной системой macOS передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства.

Сравнение параметров Агента администрирования по операционным системам

В таблице ниже описано, какие параметры политики Агента администрирования доступны в зависимости от операционной системы управляемого устройства, на котором установлен Агент администрирования.

Параметры Агента администрирования: сравнение по операционным системам

Раздел Параметры	Windows	Linux	macOS
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Приложение может получать расширенные данные политики на устройстве**	✓
Хранилища	✓	✓ Доступна функциональность: • **Информация об установленных приложениях** • **Информация о реестре оборудования**	✓ Функциональность **Информация о реестре оборудования** доступна.
Подключения → Сеть	✓	✓ Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓
Подключения → Профили соединений	✓	✓	✓
Подключения → Расписание соединений	✓	✓	✓

Раздел Параметры	Windows	Linux	macOS
Опрос сети точками распространения	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры доменов**	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры доменов**	—
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	✓	—
Обновления (точки распространения)	✓	✓	—
История ревизий	✓	✓	✓

Настройка параметров защиты управляемых приложений

Для настройки параметров защиты управляемых приложений "Лаборатории Касперского" вы можете использовать политики.

Подробнее о настройке политик Kaspersky Endpoint Security см. в соответствующей справке:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Mac

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на управляемых устройствах.

Участвуя в Kaspersky Security Network, вы соглашаетесь автоматически предоставлять "Лаборатории Касперского" информацию о работе приложений безопасности, установленных на компьютерах и мобильных устройствах, управление которыми осуществляется с помощью Open Single Management Platform. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN.

Open Single Management Platform поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Open Single Management Platform. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Open Single Management Platform использует это решение по умолчанию.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к базам данных Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в KSN. KPSN предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

  - Устройства пользователей не подключены к интернету.

  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа Kaspersky Private Security Network в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования.

Вы можете начать использование KSN или отказаться от использования KSN в любой момент.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Open Single Management Platform проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

Функциональность KSN доступна только при наличии действующей лицензии Kaspersky EDR Expert.

Чтобы настроить доступ Сервера администрирования к KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky EDR Expert не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky EDR Expert). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Kaspersky EDR Expert) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

   При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

KPSN поддерживают следующие приложения "Лаборатории Касперского":

- Kaspersky EDR Expert
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Если вы включите KPSN в Kaspersky EDR Expert, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

> Kaspersky EDR Expert не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. Под блоком **Параметры подключения** настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - TCP-порт 13111 используется для подключения к прокси-серверу KSN. Для корневого Сервера администрирования этот номер порта изменить невозможно.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт**. По умолчанию параметр выключен, используется порт TCP. Если этот параметр включен, по умолчанию используется UDP-порт 15111. Для корневого Сервера администрирования этот номер порта изменить невозможно.

7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер Включено**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   > Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.
2. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Общие** выберите раздел **Точки распространения**.
4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
6. Нажмите на кнопку **OK**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Обратите внимание, что точка распространения не поддерживает проверку подлинности управляемого устройства по протоколу NTLM.

Включение и выключение использования KSN

Использование KSN можно включить в параметрах Сервера администрирования. Чтобы включить использование KSN для интегрированных решений, его также необходимо включить его в параметрах OSMP.

Включение и выключение использования KSN в параметрах Сервера администрирования

Чтобы включить использование KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Прокси-сервер KSN включен и отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky EDR Expert и приложений "Лаборатории Касперского".

1. В зависимости от используемого решения инфраструктуры KSN, включите соответствующие переключатели.
   - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

     Теперь доступна отправка данных в KSN. При включении этого параметра, вам нужно прочитать и принять условия Положения о KSN.

- Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network [Включено]** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

  При переводе переключателя в положение **Использовать Kaspersky Private Security Network [Включено]** появится сообщение с подробной информацией о KPSN.

2. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переключите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Выключено**, чтобы выключить службу прокси-сервера KSN.

4. Нажмите на кнопку **Сохранить**.

Включение и выключение использования KSN в параметрах OSMP

Для просмотра и изменения статуса участия в KSN и KPSN в параметрах OSMP пользователям требуется одна из следующих ролей:

- Главный администратор
- Администратор SOC
- Администратор тенанта (изменение статуса доступно только для корневого клиента – для остальных тенантов в иерархии настройки применяются автоматически)

Пользователям с ролью Аудитор доступен только просмотр статуса участия в KSN и KPSN.

Для включения использования KSN в параметрах OSMP выполните следующие действия:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.

2. В разделе **Kaspersky EDR Expert** выберите режим подключения **KSN**.

3. Включите переключатель **Участие в KSN**.

4. Внимательно прочитайте Положение о KSN.

5. Если вы согласны с условиями Положения о KSN, выберите параметр **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения документа Положение о KSN** и нажмите **Принять**.

   KSN будет включен, и Open Single Management Platform будет отправлять статистические данные в KSN для анализа специалистами "Лаборатории Касперского".

6. Если вы не согласны с условиями Положения о KSN, нажмите **Отклонить**.

   KSN не будет включена.

Для включения использования KPSN в параметрах OSMP выполните следующие действия:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.
2. В разделе **Kaspersky EDR Expert** выберите режим подключения **KPSN**.
3. Включите переключатель **Участие в KPSN**.
4. Нажмите на кнопку **Загрузить**, выберите файл конфигурации KPSN (файл с расширением pkcs7 или pem) и нажмите **Открыть**.

Участие в KPSN включено.

Для выключения использования KSN или KPSN в параметрах OSMP выполните следующие действия:

1. В главном меню приложения перейдите в раздел **Параметры** → **Kaspersky Security Network**.
2. Если вы хотите отключить участие в KSN, выберите режим подключения **KSN** и выключите переключатель **Участие в KSN**.

   Участие в KSN отключено.
3. Если вы хотите отключить участие в KPSN, выберите режим подключения **KPSN** и выключите переключатель **Участие в KPSN**.

Участие в KPSN отключено.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.
3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования с предыдущей версии обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

   В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер Kaspersky Security Network (KSN). Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете, проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:

1. На устройстве точки распространения выполните команду `ps aux`, чтобы отобразить список запущенных процессов.

2. В списке запущенных процессов проверьте, запущен ли процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy` запущен, Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область применения точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все приложения** → **Администрирование** → **Службы**).

2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

Просмотр статистики работы прокси-сервера KSN

OSMP Console позволяет просматривать статистику использования прокси-сервера KSN.

Статистика включает следующие параметры:

- статус соединения с KSN;
- количество записей в кеше;
- количество пакетов, обработанных в кеше;
- количество полученных пакетов.

Если вы используете KPSN в качестве инфраструктурного решения, отображается статистика использования KPSN.

Чтобы просмотреть статистику:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN** и откройте вкладку **Статистика**.

   На вкладке отображается актуальная статистика использования прокси-сервера KSN. Статистика обновляется каждые 15 секунд.

Вы можете скопировать статистику, нажав на кнопку **Копировать в буфер обмена**.

Управление задачами защиты конечных точек

В этом разделе описаны задачи, которые используются в Open Single Management Platform.

О задачах

Open Single Management Platform управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в OSMP Console, только если для этого приложения установлен плагин управления на сервере OSMP Console.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором с помощью OSMP Console, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область задачи

Область применения задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал) или DNS-имя. Также можно выбрать устройства, обнаруженные в сети Сервером администрирования.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

  Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Создание задачи

Чтобы создать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.

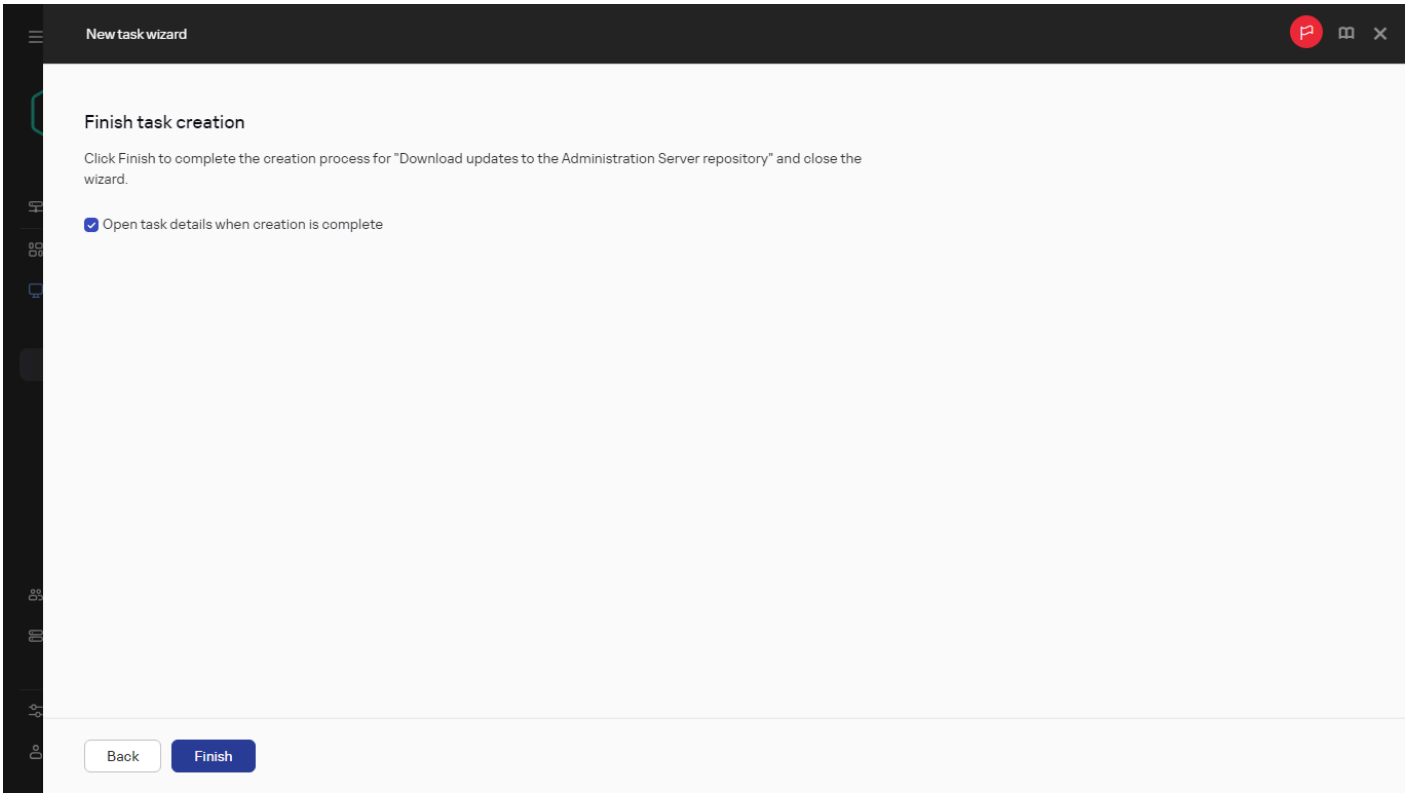
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.

3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.



Завершение создания задачи

Чтобы создать задачу, назначенную выбранным устройствам:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.

3. Нажмите на кнопку **Запустить задачу** и выберите **Создание задачи**.

   Запустится мастер создания задачи.

На первом шаге мастера вы можете удалить устройства, выбранные для включения в область действия задачи. Следуйте инструкциям мастера.

4. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

Запуск задачи вручную

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Активы (Устройства)** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.

3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

Запуск задачи для выбранных устройств

Вы можете выбрать одно или несколько клиентских устройств в списке устройств, а затем запустить для них ранее созданную задачу. Это позволяет запускать задачи, созданные ранее для заданного набора устройств.

Это действие изменит в задаче список устройств, к которым применяется эта задача.
Старая область действия задачи будет удалена и заменена на выбранную.

Чтобы запустить задачу для выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
Отобразится список управляемых устройств.

2. В списке управляемых устройств с помощью флажков выберите устройства, для которых будет выполняться задача. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.

3. Нажмите на кнопку **Запустить задачу** и выберите **Применить существующую задачу**.

Отобразится список существующих задач.

4. Выбранные устройства отображаются над списком задач. При необходимости вы можете удалить устройство из этого списка. Вы можете удалить все устройства, кроме одного.

5. Выберите необходимую задачу в списке. Вы можете использовать поле поиска над списком для поиска задачи по ее названию. Можно выбрать только одну задачу.

6. Сохраните изменения, нажав на одну из кнопок:

- **Запустить и закрыть**

  Задача запускается для выбранных устройств.

- **Запустить и открыть**

  Задача запускается для выбранных устройств и отображается окно свойств задачи, где вы можете быстро просмотреть результаты ее выполнения.

Параметры запуска по расписанию в задаче не меняются.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky EDR Expert.

Чтобы просмотреть список задач,

В главном окне приложения перейдите в раздел **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная установка приложения* относится к Серверу администрирования, а задача *Обновление* относится к Kaspersky Endpoint Security.

Чтобы просмотреть свойства задачи,

нажмите на название задачи.

Окно свойств задачи отображается с несколькими именными вкладками. Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:

  Не перезагружать устройство

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

Перезагрузить устройство

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

Принудительно закрывать приложения в заблокированных сеансах

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:

  Типы расписаний могут изменяться в зависимости от задачи.

  Некоторые типы расписаний могут быть недоступны для других приложений "Лаборатории Касперского".

  - **Параметры Запуск задачи:**

    Каждый N час

    Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

    По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

    Каждые N дней

    Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

    По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    Каждые N минут

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

    По дням недели

    Задача выполняется регулярно, в указанные дни недели, в указанное время.

    По умолчанию задача запускается каждую пятницу в 18:00:00.

    Ежемесячно

    Задача выполняется регулярно, в указанный день месяца, в указанное время.

В месяцах, у которых нет указанного дня, задача выполняется в последний день.

По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

Вручную

Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию выбран этот вариант.

Один раз

Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

Немедленно

Задача запускается сразу после сохранения ее параметров.

Ежемесячно в выбранный день

Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию указано время 18:00 и не выбраны дни месяца.

> Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

Вы можете выбрать несколько дней недели.

При загрузке обновлений в хранилище

Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи *Обновление*.

По завершении другой задачи

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

Если вы создаете для управляемого приложения задачу, расписание которой можно поставить на паузу, доступны следующие настройки расписания такой задачи:

- **Время окончания**

  Выполнение расписания задачи прекратится, начиная с 00 часов 00 минут указанной даты. При этом если в момент прекращения расписания задачи сама задача еще выполняется, ее выполнение не прерывается.

  Например, существует задача, которая запускается в 23:00 ежедневно. Вы указываете, что 1 января расписание этой задачи будет прекращено. 31 декабря задача запускается в 23:00, а 1 января в 0:00 ее расписание ставится на паузу: задача продолжает выполняться до завершения, а 1 января в 23:00 расписание больше не запускается.

  Параметр доступен для всех типов расписания, кроме **Вручную** и **Один раз**.

- **Приостановить выполнение задачи**

  Если параметр включен, вы можете задать временной интервал, в течение которого выполнение задачи, запущенной ранее по расписанию, будет приостановлено. Например, с 10:00 до 11:00.

  Это может понадобиться в период наиболее активного использования устройства чтобы снизить влияние управляемого приложения (например, Kaspersky Endpoint Security) на производительность.

  Параметр доступен для всех типов расписания.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача:

  Выбрать устройства, обнаруженные в сети Сервером администрирования

  В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

  Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  Задать адреса устройств вручную или импортировать из списка

  Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

  Назначить задачу выборке устройств

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

  Назначить задачу группе администрирования

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

- Параметры учетной записи:

  Учетная запись по умолчанию

  Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

  По умолчанию выбран этот вариант.

  Задать учетную запись

  В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  Учетная запись.

  Учетная запись, от имени которой будет запускаться задача.

  Пароль

  Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:

  Распространить на подгруппы

  Этот параметр доступен только в свойствах групповых задач.

  Когда этот параметр включен, область действия задачи включает в себя:

  - группу администрирования, которую вы выбрали при создании задачи;
  - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

  Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

  По умолчанию параметр включен.

  Распространить на подчиненные и виртуальные Серверы администрирования

  При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи – существующая и унаследованная от главного Сервера администрирования.

  Этот параметр доступен, только если параметр **Распространить на подгруппы** включен.

  По умолчанию параметр выключен.

- Дополнительные параметры расписания:

  Включать устройства перед запуском задачи функцией Wake-on-LAN

  Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

  Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

  Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

  По умолчанию параметр выключен.

  Выключать устройства после выполнения задачи

  Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

  По умолчанию параметр выключен.

  Остановить, если задача выполняется дольше

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:

  - Блок **Сохранять информацию о результатах**:

    Хранить в базе данных Сервера администрирования в течение (сут)

    События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

    По умолчанию параметр включен.

    Хранить в журнале событий ОС на устройстве

    События приложения, связанные с выполнением задачи, хранятся локально в системном журнале событий каждого клиентского устройства.

    По умолчанию параметр выключен.

    Хранить в журнале событий ОС на Сервере администрирования

    События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в системном журнале событий операционной системы Сервера администрирования.

    По умолчанию параметр выключен.

    Сохранять все события

    Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

    Сохранять события, связанные с ходом выполнения задачи

    Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

    Сохранять только результат выполнения задачи

    Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

  - **Уведомлять администратора о результатах**

    Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

    По умолчанию отключены все способы уведомлений.

  - **Уведомлять только об ошибках**

    Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

    Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности.

- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  Устройства

  Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

  Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  Выборка устройств

  Вы можете изменить выборку устройств, к которым применяется задача.

  Исключения из области действия задачи

  Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

Экспорт задачи

Open Single Management Platform позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования также недоступны для экспорта.

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

Импорт задачи

Open Single Management Platform позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу и ее параметры.

> Для корректного импорта задачи приложения "Лаборатории Касперского" нужно установить соответствующий плагин управления.

Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.

   Начнется обработка задачи.
5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:

   Назначить задачу группе администрирования

   Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

   Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

   Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   Задать адреса устройств вручную или импортировать из списка

   Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

   Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   Назначить задачу выборке устройств

   Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

   Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.
6. Укажите область действия задачи.
7. Нажмите на кнопку **Завершить**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

> Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Запуск мастера изменения паролей задач

Для не-локальной задачи, можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

Чтобы запустить мастер изменения паролей задач

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

   Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

Укажите новые учетные данные, которые в настоящее время действительны в вашей системе. При переходе на следующий шаг мастера, Open Single Management Platform проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

Использовать текущую учетную запись

Мастер использует имя учетной записи, под которой вы в настоящее время вошли в OSMP Console. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

Указать другую учетную запись

Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Open Single Management Platform заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали предыдущий пароль или указанный старый пароль не соответствует паролям, которые указаны в свойствах задач, необходимо выбрать действие, выполняемое с этими задачами.

Чтобы выбрать действие с задачей:

1. Установите флажок около задачи, с которой вы хотите выполнить действие.
2. Выполните одно из следующих действий:
   - Чтобы удалить пароль в свойствах задачи, нажмите **Удалить учетные данные**.

     Задача переключена на запуск под учетной записью по умолчанию.
   - Чтобы заменить пароль на новый, нажмите **Принудительно изменить пароль, даже если старый пароль неверен или не указан**.
   - Чтобы отменить изменение пароля, нажмите **Действие не выбрано**.

Выбранные действия применяются после перехода к следующему шагу мастера.

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky EDR Expert позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

Чтобы посмотреть результаты выполнения задачи:

в окне свойств задачи перейдите на вкладку **Результаты.**

Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.
3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Если автоматически заданное расписание задачи групповой проверки не подходит для вашей организации, вам нужно вручную настроить наиболее удобное расписание для этой задачи на основе правил рабочего процесса, принятых в организации.

Например, для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**. Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. В этом случае вам необходимо настроить задачу групповой проверки вручную.

Управление задачами обнаружения и реагирования

При работе в консоли приложения вы можете выполнять различные операции с помощью задач. Например, вы можете выполнить импорт активов или экспортировать информацию о событиях KUMA в TSV-файл.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Управление активами** → **Задачи** → **Обнаружение и реагирование**. Вы можете просматривать задачи, созданные вами (текущим пользователем).

Пользователь с ролью Главного администратора может просматривать задачи всех пользователей.

В таблице задач содержится следующая информация:

- **Статус** – статус задачи. Задаче может быть присвоен один из следующих статусов:
  - *Мигает зеленая точка* – задача активна.
  - **Завершено** – задача выполнена.
  - **Отмена** – задача отменена пользователем.
  - **Ошибка** – задача не была завершена из-за ошибки. Сообщение об ошибке отображается при наведении курсора мыши на значок восклицательного знака.
- **Задача** – тип задачи. В приложении доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий.
  - **Выполнить запрос в фоновом режиме** – выполняет SQL-запрос в фоновом режиме.
  - **Threat Lookup** – запрос данных с портала Kaspersky Threat Intelligence Portal.
  - **Ретроспективная проверка** – задание на воспроизведение событий.

- **Импорт активов OSMP** – импорт данных об активах с Серверов администрирования Kaspersky Security Center.
- **Импорт учетных записей** – импорт данных о пользователях из Active Directory.
- **Импорт активов KICS for Networks** – импорт данных об активах из KICS for Networks.
- **Обновление репозитория** - обновления репозитория KUMA для получения пакетов с ресурсами из указанного в настройках источника.
- **Резервное копирование партиций** – задача резервного копирования партиций с сохранением файла по заданному пути.
- **Восстановление партиций из резервной копии** – задача восстановления партиций из резервной копии.
- **Импорт партиций** – импорт партиций из сторонней установки KUMA.

- **Создал** – пользователь, создавший задачу. Если задача создана автоматически, в столбце указано **Задача по расписанию**.

  Этот столбец отображается только для пользователей с ролями Главный администратор и Администратор тенанта.

- **Создана** – время создания задачи.
- **Последнее обновление** – время обновления задачи.
- **Тенант** – название тенанта, в котором была запущена задача.

Формат даты задачи зависит от языка локализации, выбранного в параметрах приложения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Просмотр результатов выполнения задачи

Чтобы просмотреть результат выполнения задачи:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи** → **Обнаружение и реагирование**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Показать результат**.

Откроется окно с результатом выполнения задачи.

Повторный запуск задачи

Чтобы перезапустить задачу:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи** → **Обнаружение и реагирование**.

   Отобразится таблица задач.

2. Установите флажок рядом с задачей, которую вы хотите запустить заново.

3. Нажмите на кнопку **Перезагрузить**.

Задача будет запущена повторно.

Теги приложений

Kaspersky EDR Expert позволяет назначать теги приложениям из реестра приложений. Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств.

Например, можно создать тег `[Браузеры]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Создание тегов приложений

Чтобы создать тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Теги приложений**.

2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.

3. Укажите тег.

4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов приложения.

Изменение тегов приложений

Чтобы изменить тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените тег.
4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов приложений.

Назначение тегов приложениям

Чтобы назначить приложению теги:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.
4. Установите флажки в столбце **Назначенный тег** для тегов, которые требуется назначить.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены приложению.

Снятие назначенных тегов с приложений

Чтобы снять теги с приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.
2. Выберите приложение, с которого требуется снять теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Снимите флажки в столбце **Назначенный тег** для тегов, которые требуется снять.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную.

Удаление тегов приложений

Чтобы удалить тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Теги приложений**.

2. В списке выберите теги приложения, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в OSMP Console

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через OSMP Console, необходимо предварительно зарегистрировать его в OSMP Console.

Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:

   - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks.

     Можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования. После загрузки и установки плагина в главном меню OSMP Console отображается раздел **KICS for Networks**.

   - В веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks настраивается и включается взаимодействие с Kaspersky EDR Expert. Подробную информацию см. в справке Kaspersky Industrial CyberSecurity for Networks.

2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Нераспределенные устройства**.

   b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.

   c. Нажмите на кнопку **Переместить в группу**.

   d. В иерархии групп администрирования установите флажок рядом с группой **Управляемые устройства**.

   e. Нажмите на кнопку **Переместить**.

3. Откройте окно свойств устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

4. На странице свойств устройства в разделе **Общие** выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.

5. В окне свойств устройства выберите раздел **Приложения**.

6. В разделе **Приложения** выберите Агент администрирования Kaspersky Security Center Network.

7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас.

8. Если вы хотите просматривать статистику работы Kaspersky Industrial CyberSecurity for Networks, вы можете добавить виджеты в панель управления. Чтобы добавить виджеты, выполните следующее:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.

   b. В панели управления нажмите на кнопку **Добавить или восстановить виджет**.

   c. В появившемся виджете нажмите на кнопку **Другое**.

   d. Выберите виджет, который вы хотите добавить.

      - Карта размещения KICS for Networks
      - Информация о Серверах KICS for Networks
      - Актуальные события KICS for Networks
      - Устройства, требующие внимания в KICS for Networks
      - Критические события KICS for Networks
      - Статусы KICS for Networks

9. Чтобы перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **KICS for Networks** → **Поиск**.

   b. Нажмите на кнопку **Найти события или устройства**.

   c. В открывшемся окне **Параметры запроса** нажмите на поле **Сервер**.

   d. В раскрывающемся списке серверов, интегрированных с Kaspersky EDR Expert, выберите Сервер Kaspersky Industrial CyberSecurity for Networks и нажмите на кнопку **Найти**.

   e. Перейдите по ссылке **Перейти на Сервер** рядом с названием Сервера Kaspersky Industrial CyberSecurity for Networks.

   Откроется страница входа в Kaspersky Industrial CyberSecurity for Networks.

   Для входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks вам необходимо ввести учетные данные пользователя приложения.

Обновление баз и приложений "Лаборатории Касперского"

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky EDR Expert и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky EDR Expert и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Консоли OSMP.
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.
3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор схемы обновления**

   Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Open Single Management Platform и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования* вручную.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Open Single Management Platform. После загрузки обновлений их можно распространять на управляемые устройства.

   Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

Инструкции: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

3. **Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)**

   По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Open Single Management Platform так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

   Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

   Инструкция: Создание задачи загрузки обновлений в хранилища точек распространения

4. **Настройка точек распространения**

   Если в вашей сети назначены точки распространения, убедитесь, что параметр **Включено** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

5. **Оптимизация процесса обновления с помощью файлов различий (если требуется)**

   Вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами с помощью файлов различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования или точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Скачать файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

   Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**.

   Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

7. **Одобрение и отклонение обновлений управляемых приложений "Лаборатории Касперского"**

   По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление управляемых приложений "Лаборатории Касперского" требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для управляемого приложения было установлено, Open Single Management Platform попытается удалить обновления со всех устройств.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Консоли OSMP, и веб-плагинов управления не поддерживается.

Инструкция: Одобрение и отклонение обновлений программного обеспечения.

Иногда после обновления Агента администрирования вам может потребоваться перезагрузить управляемые устройства. Если отображается уведомление о необходимости перезагрузки, нажмите на ссылку **Просмотреть устройства** в уведомлении, установите флажки рядом с устройствами, которые требуется перезагрузить, и нажмите на кнопку **Перезагрузить**, чтобы завершить обновление Агента администрирования.

Результаты

После завершения сценария, Kaspersky EDR Expert настроен на обновление баз "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования. Теперь вы можете приступить к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

  Open Single Management Platform проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

  Open Single Management Platform позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Консоли OSMP, и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*

- С помощью двух задач:

  - Задача *Загрузка обновлений в хранилище Сервера администрирования*.

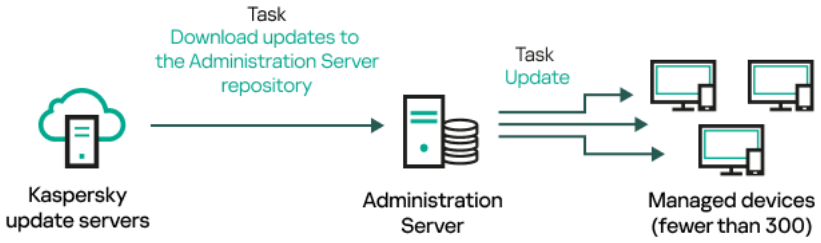
  - Задача *Загрузка обновлений в хранилища точек распространения*.

- Вручную через локальную папку, общую папку или FTP-сервер

- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

В этой схеме Open Single Management Platform загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).



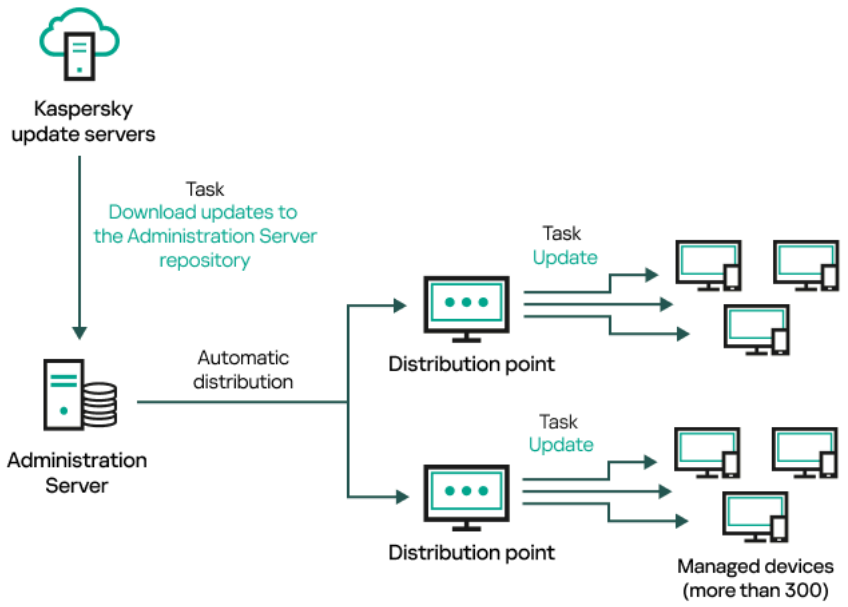
Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и без точек распространения

В качестве источника обновлений можно использовать не только серверы обновлений "Лаборатории Касперского", но и сетевую папку.

> По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* с точками распространения

После выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*, обновления баз "Лаборатории Касперского" и модули приложений для Kaspersky Endpoint Security загружены в хранилище Сервера администрирования. Эти обновления устанавливаются с помощью задачи *Обновление* Kaspersky Endpoint Security.

> Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

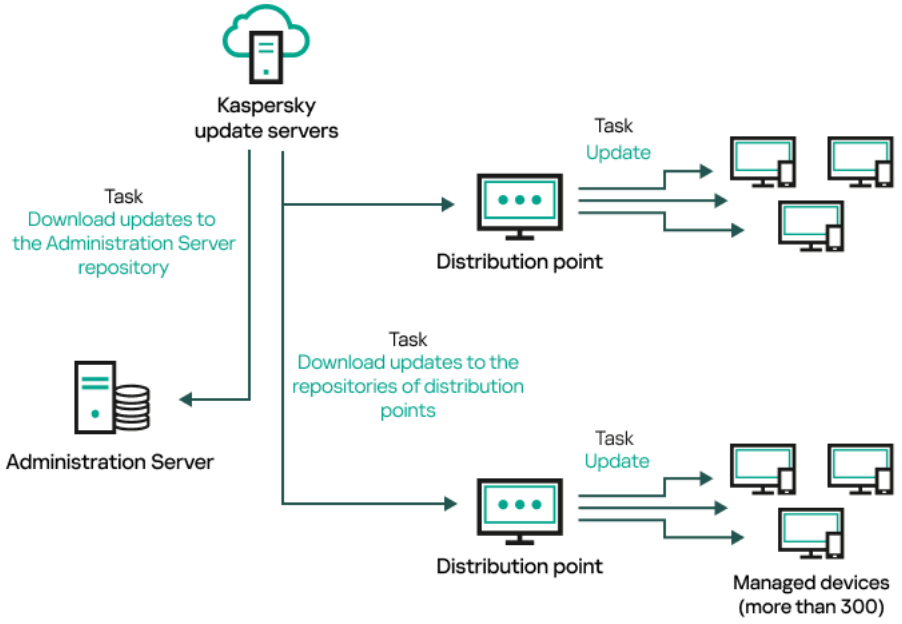
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и задачи *Загрузка обновлений в хранилища точек распространения*

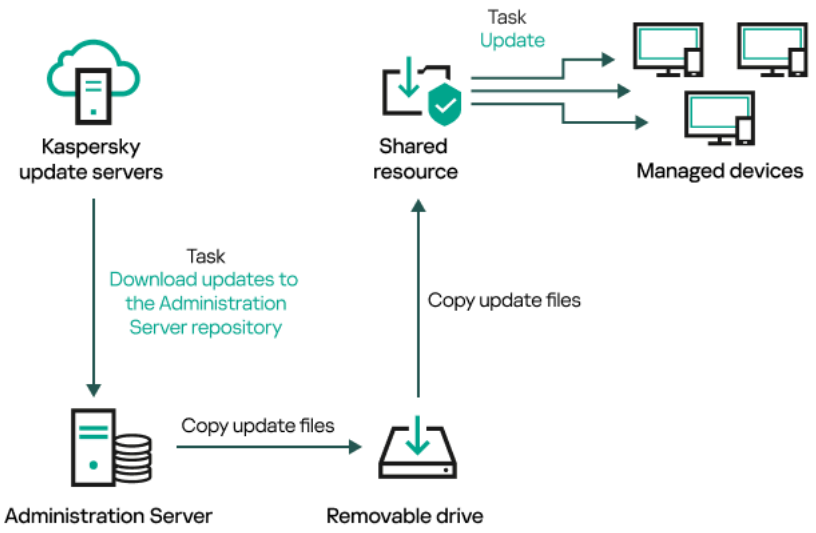
> По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Open Single Management Platform.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).



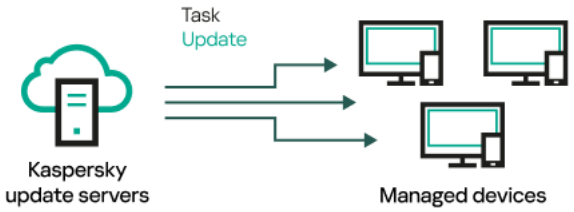
Обновление через общую папку или FTP-сервер

Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security for Linux
- Справка Kaspersky Endpoint Security for Windows

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложение безопасности не использует хранилище, предоставленное Open Single Management Platform. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в приложении безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

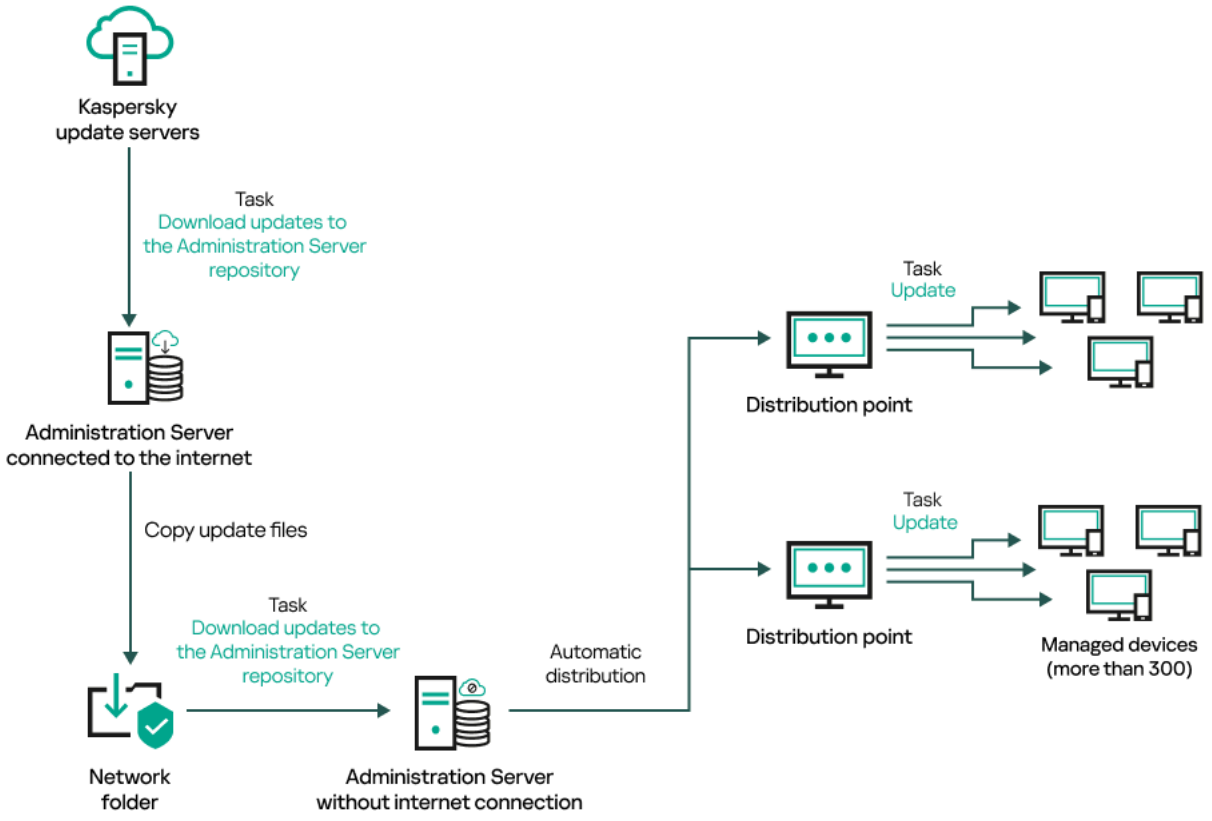
- Справка Kaspersky Endpoint Security for Linux
- Справка Kaspersky Endpoint Security for Windows

Через сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.



Обновление через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

- Kaspersky Update Utility

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр *Скачивать обновления, используя старую схему*. Вы также можете настроить параметр *Загрузить файл запроса на обновление автоматически*, чтобы утилита Kaspersky Update Utility скачивала только необходимые обновления.

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и модулей приложения безопасности "Лаборатории Касперского" с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. В списке задач может быть только одна задача *Загрузка обновлений в хранилище Сервера администрирования*.

После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* и загрузки обновлений их можно распространять на управляемые устройства.

Если вы устанавливаете Сервер администрирования в кластере, задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений*. Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы создать задачу Загрузка обновлений в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky EDR Expert выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
7. Чтобы открыть окно свойств задачи, нажмите на имя созданной задачи.

8. В окне свойств задачи на вкладке **Параметры приложения** укажите следующие параметры:

- **Источники обновлений**

  В качестве источника обновлений можно использовать серверы обновлений "Лаборатории Касперского" или сетевую папку. Если вы создаете задачу для подчиненного или виртуального Сервера администрирования, в качестве источника обновлений также можно выбрать локальную папку или главный Сервер администрирования.

  > В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Open Single Management Platform не потребует от вас ввода учетных данных.

- **Папка для хранения обновлений**

  Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Принудительно обновить подчиненные Серверы**

  Если параметр включен, Сервер администрирования будет запускать задачи получения обновлений на подчиненных Серверах администрирования сразу после получения обновлений. Задачи обновления запускаются с использованием источника обновления, который настроен в свойствах задачи на подчиненных Серверах администрирования.

  Если этот параметр выключен, задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

  По умолчанию параметр выключен.

- **Копировать полученные обновления в дополнительные папки**

  Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

  Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

  Если вы выберете копирование загруженных обновлений в локальную папку, необходимо указать на устройстве папку, которая содержит установленный Сервер администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

  При выборе сетевой папки, расположенной на Сервере администрирования с операционной системой Linux, нужно заранее обеспечить доступ к сетевой папке с устройства, на котором установлен Сервер администрирования, смонтировав папку. Доступ к папке осуществляется с использованием SMB-протокола.

По умолчанию параметр выключен.

- **Скачать файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- **Скачивать обновления, используя старую схему**

  Open Single Management Platform загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Скачивать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка, а файлы обновлений в этой папке были загружены с помощью Kaspersky Update Utility, которая загружает обновления по старой схеме.

  По умолчанию параметр выключен.

- **Выполнить проверку обновлений**

  Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

  По умолчанию параметр выключен.

- **Скачать файл запроса на обновление автоматически**

  Если вы хотите, чтобы утилита Kaspersky Update Utility скачивала только необходимые обновления с подходящей конфигурацией, включите этот параметр и укажите путь, где Kaspersky EDR Expert создаст файл запроса на обновление с информацией о скачанных обновлениях. Файл запроса на обновление содержит временную метку и MD5-хеш для контроля версий.

  Убедитесь, что параметр **Скачивать обновления, используя старую схему** выключен.

  Загрузка обновлений в Kaspersky Update Utility также должна быть настроена.

  По умолчанию указан следующий путь: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. При необходимости вы можете изменить имя по умолчанию (retranslation_request) и путь.

  > Файл запроса может быть размещен в локальной папке или в папке общего доступа. При использовании папки общего доступа вам нужно обеспечить доступ к этой папке с устройства, на котором установлен Сервер администрирования. Способы обеспечения доступа к папке и используемые инструменты зависят от вашей инфраструктуры.

При выполнении задачи *Загрузка обновлений в хранилище задачи Сервера администрирования* Kaspersky EDR Expert создает файл запроса на обновление в формате .xml по указанному вами пути. Утилита Kaspersky Update Utility автоматически получает информацию из файла запроса, а затем скачивает только необходимые обновления. Если утилита Kaspersky Update Utility не может получить информацию автоматически (например, у утилиты Kaspersky Update Utility нет доступа к папке, где приложение Kaspersky EDR Expert создало файл запроса), вам нужно передать файл с использованием сторонних инструментов.

9. В окне свойств задачи на вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск задачи**:

     - **Вручную** (выбрано по умолчанию)

       Задача не запускается автоматически. Вы можете запустить задачу только вручную.

       По умолчанию выбран этот вариант.

     - **Каждые N минут**

       Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

       По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

     - **Каждый N час**

       Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

       По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

     - **Каждые N дней**

       Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

       По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

     - **Каждую N неделю**

       Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

       По умолчанию задача запускается каждую пятницу в текущее системное время.

     - **Ежедневно (не поддерживается переход на летнее время)**

       Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

       Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky EDR Expert.

       По умолчанию задача запускается каждый день в текущее системное время.

     - **Еженедельно**

       Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно в выбранный день**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

  При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

  - Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
  - Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

    По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
  - Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

- Дополнительные параметры задачи:

  - **Запускать пропущенные задачи**

    Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

10. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются на Сервере администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Если вы используете прокси-сервер для подключения к интернету, вам нужно указать адрес прокси-сервера в свойствах Сервера администрирования. Иначе задача *Загрузка обновлений в хранилище Сервера администрирования* не будет выполняться.

Просмотр полученных обновлений

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются на Сервере администрирования. Просмотреть загруженные обновления можно в разделе **Обновления баз и модулей приложений "Лаборатории Касперского"**.

Чтобы просмотреть список полученных обновлений,

В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Приложения "Лаборатории Касперского"** → **Обновления баз и модулей приложений "Лаборатории Касперского"**.

Отобразится список доступных обновлений.

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в хранилище Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача *Проверка обновлений* завершается с ошибкой, копирование обновлений в хранилище Сервера администрирования не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;

- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО для какого-нибудь приложения, которое поддерживает Open Single Management Platform, например, Kaspersky Endpoint Security для Linux. При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Kaspersky EDR Expert проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на название задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выберите задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.
5. Если вы не создавали задачу *Проверка обновлений* ранее, выполните следующие действия:

   a. Нажмите на кнопку **Новая задача**.

   b. В открывшемся мастере создания задачи укажите название задачи, если вы хотите изменить предустановленное имя.

   c. Выберите созданную ранее группу администрирования с тестовыми устройствами.

   d. Выберите задачу обновления нужного приложения, поддерживаемого Open Single Management Platform, а затем выберите задачу поиска вредоносного ПО.

   После этого появляются следующие параметры. Рекомендуется оставить их включенными:

   - **Перезагружать устройство после обновления баз**

     После обновления антивирусных баз на устройстве рекомендуется перезагрузить устройство.

По умолчанию параметр включен.

- **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

  Если этот параметр включен, задача *Проверка обновлений* проверяет, актуальны ли обновления, загруженные в хранилище Сервера администрирования, и не снизился ли уровень защиты после обновления антивирусных баз и перезагрузки устройства.

  По умолчанию параметр включен.

e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

6. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **Сохранить**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

Создание задачи загрузки обновлений в хранилища точек распространения

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky EDR Expert;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

*Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky EDR Expert выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилища точек распространения**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.

6. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.

8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

9. На вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений для точки распространения могут быть использованы следующие ресурсы:

     - Серверы обновлений "Лаборатории Касперского"

       HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

       По умолчанию этот вариант выбран.

     - Локальная или сетевая папка

       Локальная или сетевая папка, которая содержит последние обновления. В качестве сетевой папки можно использовать только смонтированную общую папку SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

       > В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Open Single Management Platform не потребует от вас ввода учетных данных.

   - **Папка для хранения обновлений**

     Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

   - **Скачать файлы различий**

     Этот параметр включает функцию загрузки файлов различий.

     По умолчанию параметр выключен.

- **Скачивать обновления, используя старую схему**

  Open Single Management Platform загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Скачивать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка, а файлы обновлений в этой папке были загружены с помощью Kaspersky Update Utility, которая загружает обновления по старой схеме.

  По умолчанию параметр выключен.

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**:

  - **Вручную** (выбрано по умолчанию)

    Задача не запускается автоматически. Вы можете запустить задачу только вручную.

    По умолчанию выбран этот вариант.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Каждый N час**

    Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

    По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

  - **Каждые N дней**

    Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

    По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

  - **Каждую N неделю**

    Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

    По умолчанию задача запускается каждую пятницу в текущее системное время.

  - **Ежедневно (не поддерживается переход на летнее время)**

    Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

    Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky EDR Expert.

По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно в выбранный день**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и модулей приложений копируются с источника обновлений и размещаются в хранилищах точек распространения. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования

При создании или использовании задачи загрузки обновлений в хранилище Сервера администрирования, вы можете выбрать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского"
- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Сетевая папка

> В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Open Single Management Platform не потребует от вас ввода учетных данных.

Серверы обновлений "Лаборатории Касперского" используются по умолчанию, но также можно загружать обновления из локальной или сетевой папки. Можно использовать эту папку, если ваша сеть не имеет доступа к интернету. В этом случае можно вручную загрузить обновления с серверов обновлений "Лаборатории Касперского" и поместить загруженные файлы в нужную папку.

Можно указать только один путь к локальной или сетевой папке. В качестве локальной папки необходимо указать папку на устройстве, где установлен Сервер администрирования В качестве сетевой папки можно использовать FTP-сервер или HTTP-сервер или общий ресурс SMB. Если общий ресурс SMB требует аутентификации, его нужно заранее подключить к системе с необходимыми учетными данными. Не рекомендуется использовать протокол SMB1, так как он небезопасен.

Если вы добавите и серверы обновлений "Лаборатории Касперского", и локальную или сетевую папку, то сначала будут загружаться обновления из папки. В случае ошибки при загрузке будут использоваться серверы обновлений "Лаборатории Касперского".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

Чтобы добавить источники обновлений:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Загрузка обновлений в хранилище Сервера администрирования**.
3. Перейдите на вкладку **Параметры приложения**.
4. Около **Источники обновлений** нажмите на кнопку **Настроить**.
5. В появившемся окне нажмите на кнопку **Добавить**.
6. В списке источников обновлений добавьте необходимые источники. Если вы установите флажок **Сетевая папка** или **Локальная или сетевая папка**, укажите путь к папке.
7. Нажмите на кнопку **OK**, а затем закройте окно свойств источника обновлений.
8. В окне источника обновлений нажмите на кнопку **OK**.
9. Нажмите на кнопку **Сохранить** в окне задач.

Теперь обновления загружаются в хранилище Сервера администрирования из указанных источников.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

> Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, OSMP Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Приложения "Лаборатории Касперского"** → **Бесшовные обновления**.

   Отобразится список доступных обновлений.

Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. При необходимости примите Лицензионное соглашение, нажав на кнопку **Просмотреть и принять Лицензионные соглашения**.

3. Выберите обновления, которые требуется подтвердить или отклонить.

4. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky EDR Expert не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите область действия задачи.

6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.

7. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.

9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:

    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.

    - **Мобильный режим**: между устройством и Kaspersky EDR Expert не установлена связь (например, если устройство не подключено к интернету).

11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.

12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky EDR Expert.

    Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

    Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.

15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

Когда Kaspersky EDR Expert загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Включение функции загрузки файлов различий

Этапы

1. **Включение функции на Сервере администрирования**

   Включите функцию в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

2. **Включение функции для точки распространения**

Включить функцию для точки распространения, которая получает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

Включите функцию в параметрах политики Агента администрирования для точки распространения, которая получает обновления с Сервера администрирования.

Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

Эта функция включается в свойствах политики Агента администрирования и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения**.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Загрузка обновлений точками распространения

Kaspersky EDR Expert позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

Чтобы настроить получение обновлений для точки распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, через которую будут доставляться обновления на клиентские устройства в группе.

4. В окне свойств точки распространения выберите раздел **Источник обновлений**.

5. Выберите источник обновлений для точки распространения:

   Источник обновлений

   Выберите источник обновлений для точки распространения:

   - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.

   - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.

     - Если такая задача уже существует для устройства, выберите задачу в списке.

     - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   Скачать файлы различий

   Этот параметр включает функцию загрузки файлов различий.

   По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилища Сервера администрирования.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

  Чтобы хранилище Сервера администрирования содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища Сервера администрирования с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*.

- Любого устройства, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища Сервера администрирования.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.

2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Также вы можете настроить в Open Single Management Platform регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.

3. На автономных устройствах настройте Kaspersky Endpoint Security на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

   Инструкции:

   - Справка Kaspersky Endpoint Security for Linux

   - Справка Kaspersky Endpoint Security for Windows

4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.

5. На автономном устройстве, требующем установки обновлений, запустите задачу Kaspersky Endpoint Security for Linux или Kaspersky Endpoint Security for Windows *Обновление*, в зависимости от операционной системы автономного устройства.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:
   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.

4. На вкладке **Дополнительно** нажмите **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.

4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

      - **Уровень трассировки**

        Уровень трассировки определяет состав информации, которую содержит файл трассировки.

      - **Трассировка на основе ротации**

        Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

        Этот параметр доступен только для Kaspersky Endpoint Security.

   c. Нажмите на кнопку **Сохранить**.

Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

> На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security for Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security for Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security for Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

b. Выберите один из уровней трассировки Xperf:

- **Базовый тип**

  Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

  По умолчанию выбран этот вариант.

- **Тип перезагрузки**

  Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

c. Определите размер файла ротации.

d. Нажмите на кнопку **Сохранить**.

Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security for Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.

4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы трассировки устройства**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.

6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **Скачать**. Вы можете выбрать один или несколько файлов для загрузки.

   - Загрузите часть выбранного файла:

     a. Нажмите на кнопку **Скачать часть**.

     Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части файла недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.

3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   Ссылка **Журналы службы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

   Откроется окно **Журналы трассировки устройства**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Чтобы загрузить с клиентского устройства параметры приложений:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Скачать** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Информация о системе**.
3. Нажмите на кнопку **Скачать** для загрузки системной информации о клиентском устройстве.

   Если вы получаете системную информацию об устройстве под управлением Linux, в получившийся файл добавляется файл дампа для аварийно завершенных приложений.

   Архив может содержать конфиденциальные данные (например, ключи и пароли) в виде обычного текста. Рекомендуется просмотреть файлы в архиве и удалить такие данные перед отправкой в Службу технической поддержки "Лаборатории Касперского".

Файл с информацией загрузится в указанное расположение.

Загрузка журналов событий

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Все журналы устройства**.
3. В окне **Все журналы событий устройства** выберите один или несколько журналов событий.

4. Выполните одно из следующих действий:

   - Загрузите выбранный журнал событий, нажав на кнопку **Скачать весь файл**.
   - Загрузите часть выбранного журнала событий:

     a. Нажмите на кнопку **Скачать часть**.

     Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части журнала событий недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:

   - **Остановить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Перезапустить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Запустить приложение**

     Эта кнопка доступна, только если приложение в данный момент не запущено.

   В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов

Чтобы запустить диагностику Агента администрирования Kaspersky Security Center на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите **Агент администрирования Kaspersky Security Center**.

   Откроется список параметров удаленной диагностики.

4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. По завершении процесса диагностики кнопка **Скачать отчет диагностики** становится доступной.

5. Нажмите на кнопку **Скачать отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Если вы хотите запустить пользовательский скрипт на клиентском устройстве, вы можете использовать переменную среды `KLACDT_SAVE_SETTING`, чтобы определить путь, по которому будут сохранены результаты выполнения. Например:

- Для устройств с операционной системой Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Для устройств с операционной системой Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В поле **Тип объекта** выберите тип объекта, который вы хотите загрузить:

   - Выберите **Файл** для загрузки исполняемого файла.

   - Выберите **Папка** для загрузки папки, содержащей приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.

   - Выберите **Архив** для загрузки ZIP-архива, содержащего приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.

     > ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

4. Загрузите объект, выбрав его в системном окне или перетащив его в поле загрузки.

5. При необходимости в поле **Аргументы командной строки** укажите аргументы командной строки, которые будут переданы при запуске исполняемого файла.

6. Нажмите на кнопку **Загрузить и запустить** для запуска выбранного приложения на клиентском устройстве.

7. После успешного выполнения приложения, загрузите результаты выполнения, нажав на кнопку **Скачать результаты выполнения приложения**.

   > Результаты выполнения приложения хранятся до тех пор, пока вы не запустите новую диагностику или не закроете окно.

Удаленная диагностика клиентского устройства с использованием приложения завершена.

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

> Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу экспертов Службы технической поддержки. Подробная информация о требованиях к использованию утилиты kldumper приведена в Базе знаний Kaspersky Security Center.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В разделе **Формирование файла дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.

4. Нажмите на кнопку **Скачать дамп файла**.

   Архив с файлом дампа для указанного приложения загружен.

   Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

   Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Kaspersky Security Center.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Open Single Management Platform позволяет загружать основную диагностическую информацию с клиентского устройства. Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Open Single Management Platform, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz.

2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.

3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах

В этом разделе описаны возможности Kaspersky EDR Expert связанные с управлением сторонних приложений и исполняемых файлов на клиентских устройствах.

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky EDR Expert развернут в вашей организации.
- Политика Kaspersky Endpoint Security for Linux или Kaspersky Endpoint Security for Windows создана и активна. Компонент Контроль приложений включен в политике.

Этапы

Сценарий использования компонента Контроль приложений состоит из следующих этапов:

1. **Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

   Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации.

   Инструкции: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

   Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

   Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

   - *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
   - *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

   Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky EDR Expert существует три типа категорий исполняемых файлов:

   - Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
   - Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
   - Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security for Linux с использованием категорий, которые вы создали на предыдущем этапе.

   Инструкция: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

4. **Включение компонента Контроль приложений в тестовом режиме**

   Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

- Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
- Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

Инструкции для OSMP Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

5. **Изменение параметров компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию пополняемую вручную.

   Инструкции для OSMP Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений.

6. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для OSMP Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

7. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории для исполняемых файлов.
   - Настроили Контроль приложений с использованием категорий.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Режимы и категории компонента Контроль приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений. Вы можете использовать правила компонента Контроль приложений для контроля запуска приложений.

> Компонент Контроль приложений доступен для версии приложения Kaspersky Endpoint Security 11.2 для Linux и выше.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky EDR Expert существует три типа категорий:

- Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky EDR Expert выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями следующим образом:

   - Нажмите на значок параметров (⚙) в правом верхнем углу таблицы.

     В открывшемся меню **Параметры таблицы** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип ОС**.

   - Нажмите на значок фильтрации (▽) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Устройства** → **Управляемые устройства** → **имя устройства** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на клиентских устройствах, одним из следующих способов:

- Включив уведомление о запуске приложений в политике Kaspersky Endpoint Security.
- Создав задачу инвентаризации.

Включение уведомлений о запуске приложений в политике Kaspersky Endpoint Security

Чтобы включить уведомления о запуске приложения:

1. Откройте параметры политики Kaspersky Endpoint Security и перейдите на вкладку **Общие параметры** → **Отчеты и хранилища**.

2. В группе параметров **Передача данных на Сервер администрирования** установите флажок **О запущенных приложениях** и сохраните изменения.

   Когда пользователь пытается запустить исполняемые файлы, информация об этих файлах добавляется в список исполняемых файлов на клиентском устройстве. Kaspersky Endpoint Security отправляет эту информацию Агенту администрирования, а затем Агент администрирования отправляет ее на Сервер администрирования.

Создание задачи инвентаризации

Функция инвентаризации исполняемых файлов доступна для приложения Kaspersky Endpoint Security for Linux версии 11.2 и выше.

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для того чтобы сохранить место в базе данных, вам нужно запустить задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений. Предпочтительное количество устройств равно 1–3.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите Kaspersky Endpoint Security for Linux или Kaspersky Endpoint Security for Windows в зависимости от типа операционной системы клиентских устройств.

4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

   После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

Во время инвентаризации могут быть обнаружены исполняемые файлы в следующих форматах (в зависимости от выбранного вами параметра в свойствах задачи инвентаризации): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML.

Просмотр списка приложений и исполняемых файлов, хранящихся на управляемых устройствах

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

При необходимости вы можете отправить исполняемый файл управляемого устройства на устройство, где открыто приложение OSMP Console.

Чтобы отправить исполняемый файл:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Исполняемые файлы**.
2. Перейдите по ссылке исполняемого файла, который вы хотите отправить.
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

   Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования**.

4. Нажмите на кнопку **Отправить**.

   Выбранный исполняемый файл будет загружен для дальнейшей отправки на устройство, на котором открыто приложение OSMP Console.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

Чтобы создать пополняемую вручную категорию приложений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории приложений и выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.

5. На шаге **Критерии условия** выполните следующие действия:

   a. Выберите тип правила для создания категории:

   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

     Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

     > Информация о сертификатах может быть извлечена только из исполняемых файлов формата PE (.exe, .dll, .sys).

   - **Задайте путь к приложению (поддерживаются маски)**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

   - **Съемный диск**

     Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

   - **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

     - **Выберите из списка исполняемых файлов**

       Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

     - **Выберите из реестра приложений**

Если выбран этот параметр, отображается реестр приложений. После того как вы выберете приложение из реестра, откроется окно с параметрами, заполненными метаданными из выбранного вами приложения:

- Имя файла.
- Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Название приложения.
- Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Производитель.

Обратите внимание, что блокируется только запуск исполняемых файлов, соответствующих указанным параметрам, но не запуск выбранного вами приложения. Если выбранные метаданные приложения совпадают с метаданными исполняемого файла, который запускается при запуске приложения, вы можете перейти к следующему шагу. Иначе вам нужно будет изменить значения вручную, чтобы они совпадали с метаданными исполняемого файла.

- **Задайте вручную**

  Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

  Хеш файла

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории:

  - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security for Linux, установите флажок **SHA256**.
  - Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

  Метаданные

  Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Условие категории соответствует только исполняемым файлам с одинаковыми метаданными.

  Сертификат

  Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

  Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

- **Из архивной папки**

Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления приложений в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию приложений.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Для использования критериев **Метаданные** и **Сертификат** нужно вручную указать их после загрузки файла или архивной папки.

Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления приложений в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию приложений.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Для использования критериев **Метаданные** и **Сертификат** нужно вручную указать их после загрузки файла или архивной папки.

b. При необходимости добавьте комментарий в поле **Описание**. Количество символов не может превышать 1000.

Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Условия**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

> При выборе типа правила **Из KL-категории** вы можете добавить один комментарий для всех условий, которые будут созданы на основе этого типа правила. Вы можете изменить или удалить комментарий для каждого условия отдельно.

Выбранный критерий добавлен в список условий.

Вы можете добавить любое количество критериев для создаваемой категории приложений.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.

   При необходимости вы можете добавите комментарий в поле **Описание**. Количество символов не может превышать 1000.

   Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Исключения**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения работы мастера категория приложений будет создана и отобразится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Убедитесь, что выполнены следующие предварительные требования:

- Компонент Контроль приложений включен в политике Kaspersky Endpoint Security.
- Получен список исполняемых файлов, хранящихся на управляемых устройствах.

Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Категории приложений**.

   Откроется страница со списком категорий исполняемых файлов.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории** укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.

4. Нажмите на кнопку **Добавить**.

5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории приложений.

6. Задайте следующие параметры:

   - **Алгоритм вычисления хеш-функции**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

     SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

     Выберите один из вариантов вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории:

     - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security for Linux, установите флажок **SHA256**.

     Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

     По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

     По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

   - **Синхронизировать данные с хранилищем Сервера администрирования**

     Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

     По умолчанию параметр выключен.

     Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

   - **Тип файла**

     В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

     Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

     Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

  В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

  Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

  Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете создать категорию при настройке компонента Контроль приложений.

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы из выбранных папок:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Категории приложений**.

   Откроется страница со списком категорий.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky EDR Expert.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky EDR Expert.

     По умолчанию флажок снят.

- **Алгоритм вычисления хеш-функции**: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** / **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky EDR Expert для файлов категории:

  - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security for Linux, установите флажок **SHA256**.

  Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

  По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

  По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете использовать категорию для настройки компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий исполняемых файлов и параметры каждой категории.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Категории приложений**.

Откроется страница со списком категорий.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории.

Откроется окно свойств выбранной категории. Параметры сгруппированы на нескольких вкладках.

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security for Windows:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security for Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Выключите переключатель **Контроль приложений [Выключен]**, чтобы выключить параметр.

5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security for Windows блокировку запуска приложений.

   Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security for Windows не блокирует запуск приложений, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security for Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

   Информация о модуле и приложении, которое загрузило модуль, будет сохранена в отчете.

   Kaspersky Endpoint Security for Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security for Windows контролировало все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security for Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.

8. В блоке параметров **Режим Контроля приложений** выберите режим **Список запрещенных** или **Список разрешенных**.

   По умолчанию выбран режим **Список запрещенных**.

9. Перейдите по ссылке **Параметры списков правил**.

   Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию приложений. По умолчанию отображается вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **Список разрешенных**, если выбран режим **Список разрешенных**.

10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

    Откроется окно **Правило Контроля приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (или категории), которые вы создали ранее.

    Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

    Вы можете создать категорию, нажав на кнопку **Добавить**.

    Вы можете удалить категорию, нажав на кнопку **Удалить**.

13. После того как формирование списка категорий приложений завершено, нажмите на кнопку **OK**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента Контроль приложений в политиках Kaspersky Endpoint Security в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий.

   Если вы не создали выборку событий, связанную с Контролем приложений, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию приложений, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию приложений**

       Выберите этот параметр, если вы хотите создать категорию приложений на основе исполняемых файлов, связанных с событиями.

       По умолчанию выбран этот вариант.

       Если вы выбрали этот параметр, укажите имя новой категории.

     - **Добавить в существующую категорию**

       Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию приложений.

       По умолчанию вариант не выбран.

Если вы выбрали этот параметр, выберите категорию приложений, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В разделе **Тип правила** выберите следующие параметры:
  - **Правила для добавления в область действия**
  - **Правила для добавления в исключения**
- В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:
  - **Данные сертификата (или SHA256 для файлов без сертификата)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA256 для файлов без сертификата.

    По умолчанию выбран этот вариант.

  - **Данные сертификата (файлы без сертификата пропускаются)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

  - **Только SHA256 (файлы без хеша пропускаются)**

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 исполняемого файла.

  - **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

    Выберите этот параметр, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

    Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

5. Нажмите на кнопку **OK**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете

просмотреть параметры категории приложений, которую вы изменили или создали.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Параметры задачи поиска уязвимостей и требуемых обновлений

Помимо общих параметров задачи, вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

  При поиске уязвимостей и обновлений Kaspersky EDR Expert использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

  Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

  По умолчанию параметр включен.

  Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

  Если этот параметр включен, Агент обновлений Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

  Если этот параметр выключен, Агент обновлений Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

  Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

  По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент обновлений Windows на управляемом устройстве подключается к серверу обновлений для получения обновлений только в случае, если параметр **Соединяться с сервером обновлений для актуализации данных** включен в свойствах задачи *Поиск уязвимостей и требуемых обновлений* и параметр **Режим поиска Центра обновления Windows** установлен в **Активный** в параметрах политики Агента администрирования.

- Если вам не требуется, чтобы Агент администрирования инициировал соединение с источником обновлений Microsoft Windows и загружал обновления при выполнении задачи *Поиск уязвимостей*, вы можете установить для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, при этом параметр **Соединяться с сервером обновлений для актуализации данных** должен оставаться включенным. Это позволяет сохранить ресурсы и использовать ранее полученные обновления Windows для поиска уязвимостей. Вы можете использовать пассивный режим, если настроили получение обновлений Microsoft Windows другим способом. Если получение обновлений Microsoft Windows не настроено по-другому, не устанавливайте для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, так как в этом случае информация об обновлениях никогда не будет получена.

- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если для параметра **Выключен** выбрано значение **Режим поиска Центра обновления Windows**, Kaspersky EDR Expert не запрашивает информацию об обновлениях.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования Kaspersky Security Center, вам нужно сначала убедиться, что Сервер администрирования Kaspersky Security Center не используется в качестве WSUS-сервера, а затем выполнить следующие действия:

1. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

2. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

3. Синхронизировать свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Поиск уязвимостей и требуемых обновлений* на устройстве Агент администрирования с помощью службы Центра обновления Windows инициирует запрос обновлений Windows, применимых к устройству. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет поиск обновлений непосредственно с этого внешнего WSUS-сервера. Затем служба Центра обновления Windows пересылает этот список на Сервер администрирования с помощью Агента администрирования. Таким образом, Сервер администрирования имеет актуальную базу.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky EDR Expert выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky EDR Expert не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky EDR Expert выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Open Single Management Platform. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Open Single Management Platform. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

О лицензии

Лицензия – это ограниченное по времени право на использование Open Single Management Platform, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии Open Single Management Platform прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Open Single Management Platform вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

Справочное руководство OpenAPI

Справочное руководство OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную. Например, как администратор вы можете использовать OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.

- Пользовательская разработка. Используя OpenAPI, вы можете разработать клиентское приложение.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI

Примеры сценариев

Справочное руководство по OpenAPI содержит примеры сценариев Python, перечисленные в таблице ниже. Примеры показывают, как вы можете вызывать методы OpenAPI и автоматически выполнять различные задачи по защите вашей сети, например, создавать иерархию "главный/подчиненный", запускать задачи в Open Single Management Platform или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

Сопоставление пользовательских сценариев и примеров методов OpenAPI

Пример	Назначение примера	Сценарий
Журнал событий KlAkParams	Вы можете извлекать и обрабатывать данные, используя `KlAkParams` структуру данных. В примере показано, как работать с этой структурой данных. Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде.	Мониторинг и отчеты
Создание и удаление иерархии "главный/подчиненный"	Вы можете добавить подчиненный Сервер администрирования и установить таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Или вы можете исключить подчиненный Сервер администрирования из иерархии.	Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования и удаление иерархии Серверов администрирования
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений
Установка лицензионного ключа, хранящегося в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых приложений
Создание отчета об эффективных правах пользователей	Вы можете создать разные отчеты. Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета
Запуск задачи на устройстве	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную
Регистрация точек распространения для устройств в группе	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского"
Перечисление всех групп	Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее: • Получить идентификатор корневой группы "Управляемые устройства". • Переместить по иерархии групп. • Получить полную развернутую иерархию групп с их именами и вложенностью.	Настройка Сервера администрирования
Перечисление задач, запрос статистики задач и запуск задач	Вы можете ознакомиться со следующей информацией: • Историей выполнения задачи. • Текущим статусом задачи. • Количеством задач в разных статусах. Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики.	Запуск задачи вручную

Пример	Назначение примера	Сценарий
Создание и запуск задачи	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Название. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи.	Создание задачи
Перечисление лицензионных ключей	Вы можете получить список всех активных лицензионных ключей для приложений "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения о каждом лицензионном ключе, такие как имя, тип или срок действия.	Лицензирование
Создание пользовательской категории	Вы можете создать категорию приложений с требуемыми параметрами.	Создание пополняемой вручную категории приложений
Перечисление пользователей с помощью SrvView	Вы можете использовать класс SrvView для запроса подробной информации с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление пользователями и ролями пользователей

Приложения, взаимодействующие с Open Single Management Platform через OpenAPI

Некоторые приложения взаимодействуют с Open Single Management Platform через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform. Это также может быть пользовательское клиентское приложение, разработанное вами на основе OpenAPI.

Приложения, взаимодействующие с Open Single Management Platform через OpenAPI, подключаются к Серверу администрирования. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

Управление приложениями Endpoint Agent

Endpoint Agent представляет собой компонент Kaspersky EDR Expert, устанавливаемый на рабочих станциях и серверах в ИТ-инфраструктуре организации. Компонент Endpoint Agent осуществляет непрерывный мониторинг процессов, активных сетевых соединений и изменяемых файлов. При интеграции с Open Single Management Platform компонент Endpoint Agent отправляет в Open Single Management Platform следующую информацию:

- телеметрия;
- угрозы, обнаруженные приложением;
- результаты обработки обнаруженных угроз.

В качестве Endpoint Agent может использоваться одно из следующих приложений, в зависимости от операционной системы компьютера:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Управление приложением Kaspersky Endpoint Security для Windows

Подробное описание порядка управления приложением Kaspersky Endpoint Security для Windows приведено в справке:

- Установка и удаление приложения
- Установка плагина управления для Windows
- Управление Карантином
- Управление приложением с помощью командной строки

Управление приложением Kaspersky Endpoint Security для Linux

Подробное описание порядка управления приложением Kaspersky Endpoint Security для Linux приведено в справке:

- установка, удаление и обновление приложения
- Управление приложением с помощью командной строки
- Управление приложением с помощью Kaspersky Security Center

Управление приложением Kaspersky Endpoint Security для Mac

Подробное описание порядка управления приложением Kaspersky Endpoint Security для Mac приведено в справке:

- установка и удаление приложения
- Управление приложением с помощью командной строки
- Управление приложением через Консоль администрирования Kaspersky Security Center или Kaspersky Security Center Web Console и Cloud Console.

Мониторинг, отчеты и аудит

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky EDR Expert. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky EDR Expert можно настраивать функции мониторинга и параметры отчетов.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky EDR Expert.

Предварительные требования

После развертывания Kaspersky EDR Expert в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры, вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

   - новые параметры не противоречат политикам информационной безопасности вашей организации;
   - вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

2. **Настройка параметров уведомлений о событиях на клиентских устройствах**

   Инструкции:

   Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах.

3. **Выполнение рекомендуемых действий для критических и предупреждающих уведомлений**

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации.

4. **Просмотр состояния безопасности сети вашей организации**

   Инструкции:

   - Просмотр виджета Состояние защиты.
   - Генерация и просмотр отчета Отчет о состоянии защиты.
   - Генерация и просмотр отчета Отчет об ошибках.

5. **Нахождение незащищенных клиентских устройств**

   Инструкции:

   - Просмотр виджета Новые устройства.
   - Генерация и просмотр отчета Отчет о развертывании защиты.

6. **Проверка защиты клиентских устройств**

   Инструкции:

   - Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз.
   - Запуск и просмотр выборки событий Критическое.

7. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции:

   - Ограничение максимального количества событий.

8. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление виджета Используемые лицензионные ключи в панель мониторинга и его просмотр.
   - Генерация и просмотр отчета Отчет об использовании лицензионных ключей.

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. OSMP Console предоставляет следующие виды мониторинга и отчетов в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

Панель мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Выборки событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе OSMP Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования. Вы можете просмотреть отчеты об анализе аномального поведения в разделе **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**. Вы можете подтвердить обнаружение как корректное или добавить его в исключения, после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

Просмотр и подтверждение обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**.

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Виртуальный Сервер администрирования**

     Виртуальный Сервер администрирования, который управляет устройством.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Пусто – если администратор не обработал обнаружение.

   - **Количество обнаружений**

     Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

Чтобы просмотреть свойства обнаружения:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**.

2. Выполните одно из следующих действий:

   - В столбце **Имя** нажмите на ссылку с названием обнаружения, которое вы хотите просмотреть.

   - В списке обнаружений установите флажки рядом с уязвимостями, которые вы хотите просмотреть и нажмите на кнопку **Свойства**.

Откроется окно свойств выбранного обнаружения.

Вы можете подтвердить любое обнаружение из списка обнаружений правил Адаптивного контроля аномалий или в окне свойств выбранного обнаружения.

Чтобы подтвердить обнаружение:

- Выберите одно или несколько обнаружений в списке обнаружений и нажмите на кнопку **Подтвердить**.
- Откройте окно свойств выбранного обнаружения и нажмите на кнопку **Подтвердить**.

Статус обнаружения изменится на **Подтверждение**. Обнаружение исчезнет из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования.

Ваше подтверждение влияет на статистику, используемую правилами. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления в исключения Адаптивного контроля аномалий позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Чтобы добавить исключения из правил Адаптивного контроля аномалий с помощью мастера:

1. Запустите мастер одним из следующих способов:

   - В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**, выберите одно или несколько обнаружений и нажмите на кнопку **Исключить**.

     За один раз можно добавить до 1000 исключений.

     Перед добавлением обнаружения в исключения вы можете просмотреть свойства обнаружения, нажав на имя обнаружения или на кнопку **Свойства**. В открывшемся окне свойств обнаружения вы также можете нажать на кнопку **Исключить**.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**, нажмите на ссылку с нужной выборкой событий, установите флажок рядом с обнаружением, которое вы хотите исключить, и нажмите на кнопку **Исключить из Адаптивного контроля аномалий**.

   Запустится мастер добавления в исключения Адаптивного контроля аномалий. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. Выберите политики и профили политик, в которые вы хотите добавить исключения.

   Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика не будет обновлена.

3. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Статус обнаружения изменится на **Исключение**. Обнаружение исчезнет из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования. Исключение из правил Адаптивного контроля аномалий настроено и применено.

Панель мониторинга и виджеты

В этом разделе содержится информация о панели мониторинга и виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению виджетами и настройке виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Консоли OSMP: в разделе **Мониторинг** → **Панель мониторинга**.

В панели мониторинга представлены настраиваемые виджеты. Вы можете выбрать большое количество различных виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа виджета. Вы можете обновить данные виджета вручную с помощью меню в любое время.

Панель управления включает в себя вкладки **Администрирование и защита** и **Обнаружение и реагирование**, на которые вы можете добавлять виджеты.

Вкладка Администрирование и защита

Вкладка **Администрирование и защита** может содержать виджеты, которые отображают информацию о всех событиях, хранящихся в базе данных Сервера администрирования.

На вкладке **Администрирование и защита** доступны виджеты следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вкладка Обнаружение и реагирование

Вкладка **Обнаружение и реагирование** может содержать виджеты, которые отображают информацию о зарегистрированных алертах и инцидентах, а также действиях по реагированию на них. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

На вкладке **Обнаружение и реагирование** доступны виджеты следующих категорий:

- **События**
- **Активные листы**
- **Контекстные таблицы**
- **Алерты**
- **Активы**
- **Инциденты**
- **Плейбуки**
- **Источники событий**
- **Пользователи**

Виджеты администрирования и защиты

При настройке вкладки **Администрирование и защита** в панели мониторинга можно добавлять виджеты, скрывать виджеты, а также менять внешний вид или размер виджетов, перемещать виджеты и изменять параметры виджетов.

Некоторые виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

На вкладке **Администрирование и защита** в панели мониторинга доступны следующие категории виджетов и виджеты:

- **Состояние защиты**

  В группу входят следующие виджеты:

  - **История уязвимостей программного обеспечения**
  - **Количество уязвимых устройств**
  - **Распределение устройств по уровню критичности уязвимостей**
  - **Статус выбранного устройства**
  - **Состояние защиты**

- **Развертывание.**

  Эта группа включает в себя виджет **Новые устройства**.

- **Обновление.**

Эта группа включает следующие виджеты:

- **Статистика обновлений Центра обновления Windows.**
- **Распространение антивирусных баз.**
- **Активные алерты.**
- **Статистика результатов установки обновлений по категории обновления.**
- **Статистика состояния установки обновлений по категории обновления.**
- **Статистика состояния установки обновлений.**

- **Статистика угроз.**

  Эта группа включает следующие виджеты:

  - **Обнаружение угроз с помощью указанного компонента приложения, отсортированных по результатам их лечения**
  - **Обнаружение угроз компонентами приложения**
  - **Запрещенные приложения**
  - **Типы сетевых атак**
  - **Типы обнаруженных вирусов и результаты лечения**
  - **История помещения файлов на карантин**
  - **История обнаружения возможно зараженных объектов**
  - **История сетевых атак**
  - **История активности угроз по типам приложений**
  - **Активность угроз**
  - **Пользователи 10 наиболее зараженных устройств**
  - **Наиболее зараженные устройства**
  - **Самые заражаемые виртуальные Серверы**
  - **Наиболее распространенные угрозы**
  - **Наиболее заражаемые Windows-домены**
  - **Наиболее заражаемые группы**
  - **Алерты**

- **Другое**

Эта группа включает следующие виджеты:

- **Использование лицензионных ключей**
- **Уведомления, выбранные по уровню важности**
- **Десять наиболее частых событий базы данных**
- **Текущее состояние выбранной задачи Сервера администрирования**
- **История задачи**

Добавление виджета на информационную панель

Чтобы добавить виджет на информационную панель:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить виджет**.
3. В списке доступных виджетов выберите виджет, который требуется добавить на информационную панель.

   Виджеты сгруппированы по категориям. Чтобы посмотреть, какие виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.
4. Нажмите на кнопку **Добавить**.

Выбранные виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид и параметры добавленных виджетов.

Удаление виджета с информационной панели

Чтобы удалить виджет с информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется удалить.
3. Выберите **Скрыть виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **OK**.

Выбранный виджет будет удален с информационной панели. В дальнейшем можно опять добавить виджет на информационную панель.

Перемещение виджета на информационной панели

Чтобы переместить виджет на информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить виджет. Можно выбрать только другой виджет.

   Выбранные виджеты поменяются местами.

Изменение размера или внешнего вида виджета

Можно изменить внешний вид виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых виджетов можно изменить размер: маленький, средний или крупный.

Чтобы изменить внешний вид виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется изменить.
3. Выполните одно из следующих действий:
   - Чтобы виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

   Внешний вид выбранного виджета будет изменен.

Изменение параметров виджета

Чтобы изменить параметры виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется изменить.
3. Выберите **Показать параметры**.
4. В открывшемся окне параметров виджета измените требуемые параметры виджета.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Параметры выбранного виджета будут изменены.

Набор параметров зависит от конкретного виджета. Ниже приведены некоторые общие параметры:

- **Область виджета** – набор объектов, для которых виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – задача, для которой виджет отображает информацию.
- **Период** – период, за который отображается информация в виджете; например, между двумя заданными датами, от заданной даты до настоящего времени или за указанное количество дней до настоящего времени.
- **Установить статус "Критический", если** и **Установить статус "Предупреждение", если** – правила, в соответствии с которыми назначаются цвета на графике статусов.

После изменения параметров виджета вы можете обновить данные виджета вручную.

Чтобы обновить данные виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется переместить.
3. Нажмите на кнопку **Обновить**.

   Данные виджета обновлены.

Веб-виджеты обнаружения и реагирования

На вкладке **Обнаружение и реагирование** вы можете добавлять, настраивать и удалять виджеты.

Набор виджетов, используемых на вкладке **Обнаружение и реагирование**, называется *макетом*. Все веб-виджеты должны быть размещены на макетах. Kaspersky EDR Expert позволяет создавать, изменять и удалять макеты. Также доступны преднастроенные макеты панели мониторинга. При необходимости вы можете изменять параметры виджета в предварительно настроенных макетах. По умолчанию на вкладке **Обнаружение и реагирование** выбран макет **Обзор алертов**.

Веб-виджет отображает данные за период, выбранный в параметрах веб-виджета или макета, только для тенантов, указанных в параметрах веб-виджета или макета.

Перейдя по ссылке с названием виджета о событиях, алертах, инцидентах или активных листах, вы можете перейти в соответствующий раздел интерфейса Kaspersky EDR Expert. Обратите внимание, что этот параметр недоступен для некоторых виджетов.

На вкладке **Обнаружение и реагирование** в панели мониторинга доступны следующие категории виджетов и виджеты:

- **События**. Виджет для создания аналитики на основе событий.
- **Активные листы**. Виджет для создания аналитики на основе активных листов корреляторов.
- Алерты. Группа для аналитиков, которые работают с алертами. Включает информацию об алертах и инцидентах, предоставляемую Kaspersky EDR Expert.

  В группу входят следующие веб-виджеты:

  - **Активные алерты**. Количество незакрытых алертов.
  - **Активные алерты по тенантам**. Количество незакрытых алертов, сгруппированных по тенантам.
  - **Алерты по тенантам**. Количество алертов всех статусов, сгруппированных по тенантам.
  - **Неназначенные алерты**. Количество алертов, у которых нет исполнителя.
  - **Алерты по статусу**. Количество алертов со статусами *Новый*, *Открыт*, *Назначен* или *Эскалирован*. Сгруппированы по статусу.
  - **Последние алерты**. Таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в макете тенантам.
  - **Распределение алертов**. Количество алертов, созданных в течение указанного для виджета периода.
  - **Алертов по пользователям**. Количество алертов со статусом *Назначен*. Сгруппированы по имени учетной записи.
  - **Алертов по группам**. Количество алертов, назначенных каждой группе и аналитикам в каждой группе. Алерты, назначенные аналитику, учитываются в каждой группе, членом которой является этот аналитик.
  - **Алертов по уровню важности**. Количество незавершенных алертов, сгруппированных по уровню важности.
  - **Алертов по правилу**. Количество незакрытых алертов, сгруппированных по правилу корреляции.
  - **Алерты со статусами по периодам**. Количество алертов по статусу за выбранный период.
  - **Алерты по технологиям**. Название технологии для защиты, в результате проверки которой был создан алерт.
  - **Алерты по хешам**. Количество алертов, сгруппированных по хешам проверенных объектов. Поддерживаемые типы хешей: MD5 и SHA256.

- **Алерты по источнику обнаружений**. Количество алертов, сгруппированных по источнику обнаружения.
- **Алерты по имени файла**. Количество алертов, сгруппированных по имени проверяемого файла.

- **Активы**. Группа для аналитики об активах из обработанных событий. Эта группа включает следующие виджеты:
  - **Затронутые активы в алертах**. Таблица с информацией об активах и количестве незакрытых алертов, которые связаны с этими активами. Переход от виджета к разделу со списком активов недоступен.
  - **Категории затронутых активов**. Категории активов, привязанных к незакрытым алертам.
  - **Количество активов**. Количество активов, добавленных в Kaspersky EDR Expert.
  - **Активы в инцидентах по тенантам**. Количество активов в незакрытых инцидентах. Сгруппированы по тенантам.
  - **Активы в алертах по тенантам**. Количество активов в незакрытых алертах, сгруппированных по тенантам.

- Инциденты. Группа для аналитиков, которые работают с инцидентами.

  В группу входят следующие виджеты:
  - **Активные инциденты**. Количество незакрытых инцидентов.
  - **Неназначенные инциденты**. Количество инцидентов со статусом *Открыт*.
  - **Распределение инцидентов**. Количество инцидентов, созданных в течение указанного для виджета периода.
  - **Инциденты по статусам**. Количество инцидентов, сгруппированных по статусам.
  - **Инцидентов по типу**. Количество инцидентов в любом статусе, сгруппированных по типу.
  - **Активные инциденты по тенантам**. Количество незакрытых инцидентов, сгруппированных по тенантам, доступным пользователю.
  - **Все инциденты**. Количество инцидентов всех статусов.
  - **Все инциденты по тенантам**. Количество инцидентов всех статусов, сгруппированных по тенантам.
  - **Категории активов в инцидентах**. Категории активов, которые затронуты незакрытыми инцидентами.
  - **Последние инциденты**. Таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.
  - **Инциденты по пользователям**. Количество инцидентов со статусом *Назначен*. Сгруппированы по имени учетной записи пользователя.
  - **Инциденты по группам**. Количество инцидентов, назначенных каждой группе и аналитикам в каждой группе. Инциденты, назначенные аналитику, учитываются в каждой группе, членом которой является этот аналитик.
  - **Инцидентов по уровню важности**. Количество незавершенных инцидентов, сгруппированных по уровню важности.

- **Затронутые активы в инцидентах**. Количество активов в незакрытых инцидентах. Переход от виджета к разделу со списком активов недоступен.

- **Затронутые в инцидентах пользователи**. Количество пользователей, связанных с инцидентами. Переход от виджета к разделу со списком пользователей недоступен.

- **Источники событий**. Группа для аналитиков, которые работают с событиями. В группу входят следующие виджеты:

  - **Топ источников событий по количеству алертов**. Количество незакрытых алертов, сгруппированных по источникам событий.

  - **Топ источников событий по условному рейтингу**. Количество событий, для которых существует незакрытый алерт, сгруппированных по источникам событий. Группировка осуществляется по источнику событий.

    В некоторых случаях количество алертов, созданных источниками, может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события Device Product в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими параметрами являются более ресурсоемкими.

- **Пользователи**. Группа для аналитики о пользователях из обработанных событий. В группу входят следующие виджеты:

  - **Затронутые пользователи в алертах**. Количество учетных записей, связанных с незакрытыми алертами. Переход от виджета к разделу со списком пользователей недоступен.

  - **Количество пользователей AD**. Количество учетных записей в Active Directory, полученных по LDAP в течение указанного в виджете периода.

    В таблице событий, в области сведений о событиях, в окне алертов и в виджетах имена активов, учетных записей и служб отображаются вместо идентификаторов в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID. При экспорте событий в файл идентификаторы сохраняются, но в файл добавляются столбцы с именами. Идентификаторы также отображаются при наведении курсора мыши на названия активов, учетных записей или служб.
    Поиск полей с идентификаторами возможен только по идентификаторам.

- **Плейбуки**. Группа для аналитиков, которые работают с плейбуками.

  Для просмотра виджетов в этой группе у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Подтверждающий, Аудитор.

  В группу входят следующие виджеты:

  - **Статистика MTTR**. Изменение времени первого действия по реагированию на алерты и инциденты за указанный период времени (по умолчанию 30 дней). Виджет отображает столбчатую диаграмму.

Доступны следующие параметры конфигурации виджета **Статистика MTTR**:

- **Тип MTTR**:
  - **Значение**. Изменяет среднее время до первого действия по реагированию на алерт и инциденты.
  - **Минимальный**. Изменяет минимальное время до первого действия по реагированию на алерты и инциденты.
  - **Максимальный**. Изменяет максимальное время до первого действия по реагированию на алерты и инциденты.
- **Режим реагирования**:
  - **Вручную**. Изменяет время только для первых действий по реагированию вручную.
  - **Автоматически**. Изменяет время только для автоматических первых действий по реагированию.
  - **Все**. Изменяет время на все первые действия по реагированию.
- **Область действия**:
  - **Алерты**. Изменяет время до первого действия по реагированию только на алерты.
  - **Инциденты**. Изменяет время до первого действия по реагированию только на инциденты.
  - **Все**. Изменяет время до первого действия по реагированию на алерты и инциденты.

- **Автоматический и ручной запуск плейбуков**. Общее количество автоматических и ручных запусков плейбуков за определенный период. Виджет отображает столбчатую диаграмму.

  Параметр **Тип запуска** для виджета указывает, следует ли отображать только количество автоматических запусков, только запусков вручную или общее количество запусков плейбуков за определенный период.

  Для виджетов **Статистика MTTR** и **Автоматический и ручной запуск плейбуков** вы также можете установить параметр **Длина сегментов периода**. Этот параметр указывает период, в течение которого будут сгруппированы данные. Вы можете группировать данные за каждый час, каждые 4 часа или каждые 24 часа. На столбчатой диаграмме параметр **Длина сегментов периода** указывает ширину столбца.

- **Покрытие алертов и инцидентов с помощью плейбука**. Количество активных алертов и инцидентов. Вы можете выбрать, какие компоненты отображать: инциденты, алерты или все.

  На кольцевой диаграмме отображаются алерты/инциденты в следующих секторах:

  - Алерты/инциденты, для которых был запущен плейбук в режиме **Автоматический**.
  - Алерты/инциденты, для которых был запущен плейбук в режиме **Обучение**.
  - Все остальные алерты/инциденты.

- **Экономия времени с помощью плейбуков**. Экономия времени за счет запуска всех плейбуков со *статусом Успешно* или Предупреждение.

  По умолчанию виджет не отображается.

Вы можете просмотреть полный список плейбуков, нажав на имя любого виджета плейбука.

- **IOA-правила, запускающие проверку в Sandbox**. Топ 10 IOA-правил, по которым Kaspersky Anti Targeted Attack Platform наиболее часто передает файлы на проверку компоненту Sandbox.
- **Топ сработавших IOA-правила**. Топ 10 IOA-правил, наиболее часто срабатывающих в событиях и алертах, обнаруженных технологией Targeted Attack Analyzer (TAA).
- **Устройства, запускающие IOA-правила**. Топ-10 устройств, на которых IOA-правила срабатывали чаще всего.

Основные принципы работы с виджетами

Принцип отображения данных на веб-виджете зависит от типа графика. В KUMA доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).
- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.

Основные принципы работы со всеми виджетами

В левом верхнем углу виджетов отображается название виджета. По ссылке с названием виджета о событиях, алертах, инцидентах или активных листах вы можете перейти в соответствующий раздел Консоли OSMP.

Под названием виджета отображается список тенантов, для которых представлены данные.

В правом верхнем углу виджета указан период, за который отображаются данные на виджете (например, 30 дней 30д). При этом данные, отображающиеся в панели мониторинга, могут отставать от реального времени, так как они сохраняются в кеш. Вы можете просмотреть дату и время последнего обновления, наведя курсор на значок периода.

Если параметр **Показать данные за предыдущий период** включен в свойствах виджета и виджет отображает данные за относительный период, во всплывающей подсказке также отображается предыдущий период. Предыдущий период рассчитывается относительно текущего периода – из начального и конечного значения текущего периода вычитается продолжительности текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

Вы можете изменить период отображения данных на виджете, нажав на значок периода и выбрав точную дату или относительный период в открывшемся окне. Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Время на виджете приводится в соответствие с локальным часовым поясом, установленном в браузере.

Слева от значка периода отображается кнопка **CSV**. Вы можете скачать данные, которые отображаются на виджете, в формате CSV (кодировка UTF-8). Имя скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

виджет отображает данные за период, выбранный в параметрах виджета или макета, только для тенантов, указанных в параметрах виджета или макета.

Если вы при настройке виджета включили переключатель **Итоговые значения**, на виджете отображается значение **Всего**, но при выгрузке виджета в формате CSV значение **Всего** не отображается. Для отображения значения **Всего** в отчете, вы можете воспользоваться формулами Excel или переписать итоговое значение с виджета.

Основные принципы работы с графиками типа Круговая диаграмма

Под списком тенантов отображается круговая диаграмма с легендой. В легенде отображаются названия категорий, соответствующих секторам диаграммы. Из контекстного меню категории в легенде можно перейти в раздел Консоли OSMP с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Под значком периода отображается количество событий, активных листов, активов, алертов или инцидентов, сгруппированных по выбранным критериям за период отображения данных на виджетах.

Примеры:

- На виджете **Алерты по статусу** под значком периода отображается количество алертов, сгруппированных по статусам **Новый**, **Открыт**, **Назначен** или **Эскалирован**.
  Если вы хотите просмотреть в легенде алерты только со статусами **Открыт** и **Назначен**, вы можете снять флажки слева от статусов **Новый** и **Эскалирован**.
- На виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10`, под значком периода отображается 10 событий, сгруппированных по имени и отсортированных в порядке убывания.
  Если вы хотите просмотреть в легенде события с определенными именами, вы можете снять флажки слева от имен событий, которые не должны отображаться в легенде.

Основные принципы работы с графиками типа Счетчик

На графиках этого типа отображается сумма выбранных данных.

Пример 1
На виджете **Количество активов** отображается общее количество активов, добавленных в KUMA.
Пример 2
Если вы хотите посмотреть тренды для сравнения текущих данных с данными за прошлый период, вы можете создать виджет с отображением восходящих или нисходящих трендов. Тренды настраиваются в следующих виджетах:

- **Активы → Количество активов**.
- **Активы → Пользовательский виджет**.
- **Алерты → Активные алерты**.
- **Алерты → Неназначенные алерты**.
- **Инциденты → Активные инциденты**.
- **Инциденты → Неназначенные инциденты**.
- **Инциденты → Все инциденты**.
- **Пользователи → Количество пользователей AD**.
  Чтобы настроить отображение трендов, необходимо включить переключатель **Показать данные за предыдущий период**, а затем выбрать тренд на вкладке Внешний вид. Если значение в процентах не может быть вычислено или если значения равны, отображается значок `—`. Если выбран параметр **Восходящий - лучше**, зеленая стрелка на графике указывает на восходящий тренд, красная – на нисходящий. Если выбран параметр **Нисходящий - лучше**, красная стрелка на графике указывает на восходящий тренд, зеленая – на нисходящий.
  Если вам нужно изменить отображение данных на виджете (например, вместо процентов посмотреть абсолютные значения), вы можете нажать кнопкой мыши на значение. Эта функция доступна при отображении виджета на панели мониторинга и при включенном режиме ТВ.

Основные принципы работы с графиками типа Таблица

На графиках этого типа данные отображаются в виде таблицы.

Пример:
На виджете **События**, для которого указан SQL-запрос `SELECT TenantID, Timestamp, Name, DeviceProduct, DeviceVendor FROM `events` LIMIT 10`, отображается таблица событий со столбцами **TenantID**, **Timestamp**, **Name**, **DeviceProduct**, **DeviceVendor**. Таблица содержит 10 строк.

Вы можете настроить отображение данных в таблице с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, какого цвета маркер будет добавлен в ячейку выбранного столбца. Столбец задается в раскрывающемся списке **Поле с индикатором градиента**.

Основные принципы работы с графиками типа Столбчатая диаграмма

Под списком тенантов отображается столбчатая диаграмма с легендой. В легенде отображаются названия категорий, соответствующих столбцам диаграммы. Из контекстного меню категории в легенде, вы можете перейти в раздел Консоли OSMP с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Пример:
На виджете **Netflow top internal IPs**, для которого указан SQL-запрос `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10`, на оси X диаграммы отображается сумма трафика в байтах, на оси Y диаграммы отображаются адреса портов назначения. Данные сгруппированы по адресам назначения в порядке убывания суммы трафика.

Вы также можете настроить отображение столбцов диаграммы с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, как будут окрашены столбцы диаграммы.

Основные принципы работы с графиками типа Календарная диаграмма

Под списком тенантов отображается календарная диаграмма с легендой. В легенде отображаются названия категорий, соответствующих столбцам диаграммы. Из контекстного меню категории в легенде, вы можете перейти в раздел Консоли OSMP с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Если при создании виджета с графиком типа **Календарная диаграмма** выбран вид диаграммы **Столбчатая диаграмма**, вы можете настроить отображение столбцов диаграммы с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, как будут окрашены столбцы диаграммы.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `value`
FROM `events`
GROUP BY Timestamp
ORDER BY `metric` DESC
LIMIT 250
```

На диаграмме по оси X отсчитывается дата создания события, по оси Y диаграммы отображается количество событий. Столбцы диаграммы расположены слева направо в порядке убывания количества событий.

Если в SQL-запросе используется дополнительное поле с псевдонимом `category`, столбчатая диаграмма отображается в виде сложенной диаграммы. В этом случае градиентная заливка не применяется.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, Type AS `value`
FROM `events`
GROUP BY Timestamp, Type
ORDER BY metric DESC
LIMIT 250
```

На диаграмме по оси X отображаются временные интервалы, по оси Y – количество событий. Каждая часть столбца соответствует значению поля, отмеченного как **Type**.

Если при создании виджета с графиком типа **Календарная диаграмма** выбран вид диаграммы **Линейная диаграмма**, возможны два варианта отображения графика: одна линия (если в запросе указаны только поля `metric` и `value`) и несколько линий (если используется дополнительное поле с псевдонимом `category`). Это позволяет сравнивать между собой значения по различным группам, в зависимости от того, по какому полю выполняется группировка в запросе. Например, это могут быть корреляционные правила, пользователи, устройства. Градиентная заливка к такому графику не применяется.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, CorrelationRuleName AS `value`
FROM `events`
WHERE Type = 3
GROUP BY Timestamp, CorrelationRuleName
ORDER BY metric DESC
LIMIT 250
```

На диаграмме по оси X отображаются временные интервалы (поле, отмеченное как `category`). По оси Y отображается количество срабатываний правил корреляции (поле, отмеченное как `metric`). Каждая линия на графике соответствует уникальному значению поля `value` (в этом случае, названию правила корреляции).

Для группировки вы можете использовать в календарной диаграмме следующие поля времени:

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> Для полноценной работы с данными, рекомендуется округлять с помощью поддерживаемых функций ClickHouse значения в поле времени (отмеченное как **Timestamp**) до нужного временного интервала (например, 1 час, 1 день).

Для виджета с графиком типа **Календарная диаграмма** с видом диаграммы **Линейная диаграмма** вы также можете настроить параметры для отображения среднего значения. Для этого на вкладке **Внешний вид** для параметра **Регрессия** требуется выбрать **LOESS**.

Основные принципы работы с графиками типа Линейная диаграмма

Под списком тенантов отображается линейная диаграмма с легендой. В легенде отображаются названия категорий, соответствующих линиям на графике. Из контекстного меню категории в легенде, вы можете перейти в раздел Консоли OSMP с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Пример:

На виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250`, на оси X диаграммы представлен примерный номер порта, на оси Y диаграммы отображаются количество событий. Данные сгруппированы по номеру порта в порядке возрастания.

Для виджета с графиком типа **Линейная диаграмма** вы также можете настроить параметры для отображения среднего значения. Для этого на вкладке **Внешний вид** для параметра **Регрессия** требуется выбрать **Линейная**. Если на графике отображается несколько категорий, для каждой категории отображается среднее значение.

Основные принципы работы с графиками типа Сложенная столбчатая диаграмма

Под списком тенантов отображается сложенная столбчатая диаграмма с легендой. В легенде отображаются названия категорий, составляющих части каждого столбца. Слева от каждой категории находится флажок, с помощью которого можно скрыть или показать категорию. Количество столбцов на диаграмме соответствует количеству значений в выбранной группировке. Столбцы подписаны метками. Цвет соответствующей категории в столбце присваивается автоматически. При наведении курсора мыши на области столбца отображается подсказка со значением и описанием значения. Из контекстного меню категории в легенде можно перейти в раздел Консоли OSMP с соответствующими данными.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Столбцы имеют разную интерпретацию высоты в зависимости от значения параметра **Формат**:

- Если выбран формат **Абсолютные значения**, то высота столбцов соответствует сумме значений измеряемого показателя.

- Если выбран формат **Относительные значения, %**, то все столбцы имеют одинаковую высоту 100%, а размеры подкрашенных областей столбца соответствуют процентному соотношению между значениями показателя.

Если при создании пользовательского виджета на основе сложенной столбчатой диаграммы выбран параметр **Показывать данные за предыдущий период** и в запросе указаны стандартные псевдонимы `value`, `category`, `metric`, то на диаграмме отдельными столбцами показываются данные предыдущего периода. Если же в запросе вместо стандартной метрики `metric` применяется пользовательский расчет метрик с нестандартными псевдонимами, то параметр **Показывать данные за предыдущий период** не будет учитываться при построении диаграммы (см. примеры запросов ниже).

Примеры:
При создании пользовательского виджета с графиком типа **Сложенная столбчатая диаграмма** на основе SQL-запроса для виджета **События** действуют следующие правила:

- Поле в запросе, отмеченное как псевдоним `value` (должно быть указано обязательно), будет использоваться на диаграмме как поле, по которому строится легенда и столбцы делятся на категории.
- Поле в запросе, отмеченное как псевдоним `category` (должно быть указано обязательно), будет использоваться на диаграмме как поле, по значениям которого будут расположены столбцы по оси X.
- Поле в запросе, отмеченное как псевдоним `metric`, будет использоваться на диаграмме как поле, по которому должен вестись количественный подсчет частей столбцов. В этом случае количественное распределение будет производиться автоматически.

При этом вы можете самостоятельно управлять подсчетом, используя в качестве метрик стандартные функции агрегации `sum`, `avg`, `min`, `max`, `count` и собственные псевдонимы с произвольным названием вместо стандартного псевдонима `metric` (в этом случае не будет поддерживаться отображение данных за предыдущий период).

Пример 1:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами, при создании виджета выбран параметр **Показывать данные за предыдущий период**:

```
SELECT count(ID) AS `metric`,

Type AS `value`,

TenantID AS `category`

FROM `events`

GROUP BY value, category

ORDER BY metric DESC
```

На диаграмме по оси X отображаются соответствующие тенанты (поле, отмеченное как `category`), по оси Y отображается количество событий определенного типа (поле, отмеченное как value). В каждом столбце количество, соответствующее определенному типу, отображается отдельным цветом. В легенде в качестве категорий отображаются названия типов событий, по которым разбиваются столбцы. Каждой категории соответствует цвет, автоматически присвоенный ей на столбце. Если вы хотите просмотреть на диаграмме события только с определенными типами, вы можете снять или установить флажки слева от соответствующих типов событий в легенде.

Рядом с каждым столбцом отображается дополнительный столбец с данными за прошлый период, если такие данные получены в запросе.

Пример 2:
В виджете **События** указан следующий SQL-запрос с пользовательскими метриками, отмеченными как псевдонимы `Base` и `Audit` вместо стандартного `metric`:

```
SELECT SUM(IF (Type = 1,1,0)) AS `Base`,

SUM(IF (Type = 4,1,0)) AS `Audit`,

TenantID as `category`

FROM `events`

GROUP BY category
```

На диаграмме по оси X отображаются соответствующие тенанты (поле, отмеченное как `category`), по оси Y отображается количество событий каждого типа (пользовательские метрики, отмеченные как псевдонимы Base и Audit). В каждом столбце количество, соответствующее определенной метрике, отображается отдельным цветом. В легенде в качестве названий категорий отображаются метрики `Base` и `Audit`, по которым столбцы делятся на категории. Каждой категории соответствует цвет, автоматически присвоенный ей на столбце. Если вы хотите просмотреть на диаграмме события, соответствующие только определенной метрике, вы можете снять или установить флажки слева от нужной метрики в легенде.

Дополнительный столбец с данными за прошлый период для запроса с пользовательскими метриками не отображается, даже если при создании виджета выбран параметр Показывать данные за предыдущий период.

Пример 3:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами:

```
SELECT count(ID) AS `metric`,

TenantID as `value`,

Type as `category`
```

```
FROM events

GROUP BY value, category

ORDER BY metric DESC
```

В отличие от схожего запроса в примере 1, в этом случае на диаграмме по оси X отображаются соответствующие типы событий (поле, отмеченное как `category`), а тенантам (поле, отмеченное как `value`) соответствуют области значений в столбцах (по оси X) и соответствующие подписи в легенде.

Пример 4:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами:

```
SELECT count(ID) AS `metric`,

CAST(fromUnixTimestamp64Milli(Timestamp) AS DATE) AS `category`,

Type as `value`

FROM `events`

GROUP BY category, value

ORDER BY category DESC
```

На диаграмме по оси X отображаются дни месяца (поле, отмеченное как `category`). По оси Y отображается количество событий определенного типа (поле, отмеченное как `value`).

Чтобы построить подобный график с расположением столбцов по дате и/или времени, используйте в запросе группировку и сортировку по следующим полям с типом `timestamp`:

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> Для полноценной работы с данными, расположенными по дате и/или времени, рекомендуется использовать тип графиков **Календарная диаграмма**.

Основные принципы работы с графиками типа Спидометр

На графиках этого типа отображается процентное отношение количества объектов выбранной категории к общему количеству объектов за определенный период. **Спидометр** строится для следующих объектов:

- для активов в выбранной категории, удовлетворяющих заданному условию, относительно общего количества активов в этой категории или некатегоризированных активов;
- для удовлетворяющих заданному условию алертов относительно общего количества алертов за определенный период;
- для удовлетворяющих заданному условию инцидентов относительно общего количества инцидентов;
- для удовлетворяющих заданному условию событий относительно общего количества событий за определенный период.

Значение на графике отображается в процентах с цветовой градацией по настроенным интервалам значений. По умолчанию указаны следующие интервалы процентных значений: 0–30, 30–70, 70–100.

Пример 1:
На пользовательском виджете **Активы** пользователь выбирает категорию активов, количество активов в которой сравнивается с общим количеством активов. Пользователь может указать пороговые значения для шкалы на графике. Затем на основе одного или нескольких условий для оси Y осуществляется расчет по имеющейся базе активов.

Пример 2:
На виджете **Алерты** тип **Спидометр** можно выбрать для категорий **Активные алерты** и **Неназначенные алерты**. Для алертов выбираются тенант и период для анализа. По умолчанию эти значения соответствуют значениям, указанным в применимой панели мониторинга. В общем количестве алертов можно также показать данные за предыдущий период.

Аналогичным образом рассчитывается процентное значение для категорий **Активные инциденты** и **Неназначенные инциденты** на виджете **Инциденты**.

Пример 3:
На виджете **События** для типа **Спидометр** пользователь указывает тенанта, период для анализа, а также хранилище данных о событиях. SQL-запрос к базе данных отображается в следующем виде:

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

Особенности отображения данных в виджетах

Ограничение отображаемых данных

Для удобства восприятия информации в KUMA заданы ограничения на отображение данных в виджетах в зависимости от их типа:

- Круговая диаграмма – отображается не более 20 отсеков.
- Столбчатая диаграмма – отображается не более 40 столбцов.
- Таблица – отображается не более 500 записей.
- Календарная диаграмма – отображается не более 365 дней.

Данные, выходящие за указанные ограничения, отображаются в виджете в категории **Остальное**.

Все данные, по которым построена аналитика в виджете, можно скачать в формате CSV.

Суммирование данных

Формат отображения итоговой суммы данных на календарной, столбчатой и круговой диаграммах зависит от языка локализации:

- Английская локализация: порядки разделяются запятыми, дробная часть отделяется точкой.
- Русская локализация: порядки разделяются пробелами, дробная часть отделяется запятой.

Создание виджета

Вы можете создать виджет в макете панели мониторинга во время создания или изменения макета.

Чтобы создать виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Создайте макет или переключитесь в режим редактирования для выбранного макета.
3. Нажмите на кнопку **Добавить виджет**.
4. В раскрывшемся списке выберите тип виджета.

   Откроется окно с параметрами виджета.
5. Измените параметры виджета.
6. Если вы хотите увидеть, как данные будут отображаться в виджете, нажмите на кнопку **Предварительный просмотр**.
7. Нажмите на кнопку **Добавить**.

Виджет появится на макете в панели мониторинга.

Изменение виджета

Чтобы изменить виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку Изменить ( ).

   Откроется окно **Настройка макета**.
5. В виджете, который вы хотите изменить, нажмите на значок параметров ( ).
6. Выберите **Изменить**.

   Откроется окно с параметрами виджета.

7. Измените параметры виджета.

8. Нажмите на кнопку **Сохранить** в окне свойств виджета.

9. Нажмите на кнопку **Сохранить** в окне **Настройка макета**.

   Виджет изменен.

Удаление виджета

Чтобы удалить виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Раскройте список в правом верхнем углу окна.

3. Наведите курсор мыши на соответствующий макет.

4. Нажмите на кнопку Изменить ( ).

   Откроется окно **Настройка макета**.

5. В виджете, который вы хотите удалить, нажмите на значок параметров ( ).

6. Выберите пункт **Удалить**.

7. В открывшемся окне подтверждения нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**.

   Виджет удален.

Параметры виджетов

Этот раздел содержит описание параметров всех доступных в KUMA виджетов.

Виджет События

Вы можете использовать виджет **События** для получения необходимой аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, расположенные на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Тип графика. Доступны следующие типы графиков: • **Круговая диаграмма** • **Столбчатая диаграмма** • **Счетчик** • **Линейная диаграмма** • **Таблица** • **Календарная диаграмма** • **Сложенная столбчатая диаграмма** • **Спидометр**
Формат	Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. Параметр доступен для графика типа **Сложенная столбчатая диаграмма**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата Относительные значения, % все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Вид временной диаграммы	Формат отображения временных данных: **Столбчатая диаграмма** или **Линейная диаграмма**. Параметр доступен для графика типа **Календарная диаграмма**. При выборе формата **Столбчатая диаграмма** данные по умолчанию отображаются в виде вертикальных столбцов. Если SQL-запрос содержит дополнительное поле с псевдонимом category, столбчатая диаграмма будет представлена в виде сложенной диаграммы, то есть с разбивкой каждого столбца по значениям этого поля. При выборе формата **Линейная диаграмма** данные отображаются в виде одной или нескольких (в зависимости от запроса) ломаных линий, соединяющих точки на временной оси. По умолчанию выбран формат **Столбчатая диаграмма**.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Показывать данные за предыдущий период	Включение отображения данных сразу за два периода: за текущий и за предыдущий. При использовании графика типа **Сложенная столбчатая диаграмма** параметр **Показывать данные за предыдущий период** будет учитываться, если в запросе указаны стандартные псевдонимы `value`, `category`, `metric`. Если же в запросе вместо стандартной метрики metric используется пользовательский расчет метрик с нестандартными псевдонимами, то параметр **Показывать данные за предыдущий период** учитываться не будет.
Доступные переменные	Локальные или глобальные переменные, которые вы можете использовать для фильтрации данных виджета. Нажмите на кнопку **Добавить**. Если вы добавляете локальную переменную, введите произвольное имя переменной, затем укажите значение переменной. Если вы добавляете глобальную переменную, выберите из списка имя переменной, которую вы указали в свойствах панели мониторинга.
Хранилище	Хранилище, в котором выполняется поиск событий. В списке отображаются доступные пространства. Можно выбрать только одно хранилище, можно выбрать одно или несколько пространств. Значения в поле **Хранилище** не зависит от выбранных тенантов в поле **Тенант**. В поле отображаются хранилища и пространства, как в разделе **События**. Если в хранилище было создано новое пространство, в параметрах виджета новое пространство по умолчанию не выбрано. Следует выбрать новое пространство вручную. Если у пользователя есть доступ ко всем пространствам, указанным в виджете, тогда на виджете будут доступны для просмотра данные по событиям тенантов, указанным в наборе пространств и в правах пользователя. Если у пользователя нет прав доступа к одному или нескольким пространствам хранилища, данные на виджете будут недоступны для просмотра, пользователь не может изменить виджет, но может продублировать виджет с помощью кнопки **Дублировать**. Дублирование не зависит от прав доступа к пространствам. При дублировании шаблона в тех виджетах, где были указаны недоступные пользователю пространства, значение в поле **Хранилище** будет сброшено. В таких виджетах будет отображаться ошибка Access denied (Operation returns no results because of allowed and selected event spaces). Для сохранения шаблона необходимо указать пространства в виджетах. В тех виджетах, где были указаны пространства, доступные пользователю, значение поля **Хранилище** не сбрасывается и сохраняется при дублировании шаблона. При выгрузке отчета пользователь получит файл, в котором скрыты данные недоступных виджетов. Если адрес электронной почты пользователя указан в списке получателей отчета по расписанию, пользователь получит полную версию отчета независимо от доступных пространств.

Параметр	Описание

Поле SQL-запроса	Запрос для фильтрации и поиска событий вручную. Вы можете составить запрос в конструкторе запросов, нажав на кнопку **Использовать конструктор SQL**.
	
	Вы можете использовать поля расширенной схемы событий для построения графика типа **таблица**.
	
	Пример
	
	Предварительное условие
	Из FWSaaS-системы поступают события.
	10.08.2023 12:12:12 src=10.10.10.10 ReqUrls=[https://google.com, https:/ya.ru]
	10.08.2023 12:12:23 src=10.10.10.20 ReqUrls=[https://google.com, https:/yandex.ru]
	10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru]
	Главный администратор KUMA добавил поле расширенной схемы событий в разделе KUMA **Параметры** → **Другое** → **Поля расширенной схемы событий**. В нормализаторе KUMA настроено сопоставление полей **ReqUrls** и **SA.urls**.
	В KUMA нормализованные события выглядят следующим образом:
	DeviceReceiptTime=10.08.2023 12:12:12 SourceAddress=10.10.10.10 SA.urls=[https://google.com, https:/ya.ru]
	DeviceReceiptTime=10.08.2023 12:12:23 SourceAddress=10.10.10.20 SA.urls=[https://google.com, https:/yandex.ru]
	DeviceReceiptTime=10.08.2023 12:12:30 SourceAddress=10.10.10.30 SA.urls=[https://google.com, https:/ya.ru, https://mail.ru]
	Вы хотите построить панель мониторинга Top URLs за 30 мин. Пример запроса в разделе **События** и в виджетах:
	SELECT res.1 AS url, res.2 AS count FROM (SELECT arrayJoin(groupArray((url, count))) AS res FROM (SELECT url, count() AS count FROM (SELECT SA.urls AS urls FROM `events`) ARRAY JOIN urls AS url GROUP BY url) GROUP BY url)
	Результаты:
	url count
	google.com 3
	ya.ru 2
	mail.ru 1
	yandex.ru 1
	
	KUMA поддерживает следующие виды функций, которые позволяют использовать массивы в запросах:
	• Функция `groupArray` упаковывает все значения аргумента x в массив и используется в агрегатных функциях при группировке данных.
	• Функция `arrayJoin` разделяет массив на отдельные строки по запросу.
	При составлении SQL-запроса вы можете использовать переменные. Переменные можно указывать только при составлении запроса вручную. В конструкторе SQL переменные невозможно использовать.
	
	Пример с использованием переменных
	
	Пример SQL-запроса с использованием локальной переменной:
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	В этом запросе использована локальная переменная `$Name`. В эту переменную будет подставляться значение из **поля события Name**. Вы сможете применить переменную, нажав на значок воронки ( ) на виджете. В открывшемся окне вы сможете выбрать значение для переменной. Виджет отфильтрует выборку по выбранному значению поля **Name**.
	Обратите внимание, если в SQL-запросе вы прописываете переменную для поля, которое принимает числовое значение, такое значение надо преобразовать в строку. Для этого используйте функцию `toString`. В противном случае SQL-запрос вернет ошибку.
	Пример:
	`SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	В этом запросе **поле события SourcePort имеет числовое значение**, поэтому оно преобразовано в строку: `toString(SourcePort)`.
	
	Подробнее о создании SQL-запроса в конструкторе запроса см. ниже.
	
	Существуют следующие ограничения:
	• Псевдонимы `metric` и `value` в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по событиям, кроме таблиц.
	• Псевдонимы в виджетах с графиком типа **Таблица** могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"Псевдоним с пробелом"`, `` `Другой псевдоним` ``.
	• Не поддерживается использование `SQL-запроса ARRAY JOIN`.
	• При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.
	• В виджетах с графиком типа **Счетчик** для значений функции `SELECT` требуется указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`.
	• В виджетах с графиком типа **Таблица** градиент строится по значениям числового или временного поля (например, `Timestamp`), указанного в SQL-запросе. Это поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента** (если в запросе указано несколько числовых или временных полей, они все будут доступны для выбора). После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Если поле отсутствует в запросе, на вкладке **Внешний вид** не отображаются поля **Градиент** и **Поле с индикатором градиента**.
	• В виджетах с графиком типа Сложенная столбчатая диаграмма значения временного поля `Timestamp` не отображаются по оси X при использовании стандартного запроса. Если требуется отображать время по оси X, рекомендуется использовать график типа **Линейная диаграмма**. Если вам нужно использовать график типа **Сложенная столбчатая диаграмма**, значение `Timestamp` необходимо конвертировать в строку `toString(Timestamp) AS `category``.

Настройка значения периода

Чтобы настроить период отображения данных, выполните одно из следующих действий:

- При необходимости измените дату и время в параметре **Период** одним из следующих способов:

  - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

    Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

  - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

    Период рассчитывается относительно настоящего времени.

  - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

    Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

    В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

    > Поле **Дата от** является обязательным, и его значение не может превышать значение, установленное в поле **Дата до**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **Дата до**, параметр **now** указывается автоматически.

  Время в KUMA хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

  Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

Границы периода включаются: например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 UTC до 00:00:00:000 UTC сегодняшнего дня. Вы можете посмотреть дату и время последнего обновления данных и точный период, за который отображаются данные, наведя курсор на значок периода на виджете.

Если параметр Показать данные за предыдущий период включен в свойствах виджета и виджет отображает данные за относительный период, во всплывающей подсказке также отображается предыдущий период. Предыдущий период рассчитывается относительно текущего периода – из начального и конечного значения текущего периода вычитается продолжительности текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

- Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Как создать запрос в конструкторе запросов

Чтобы создать запрос в конструкторе запросов:

1. Укажите значения для следующих параметров:

   a. **SELECT** – поля событий, которые следует возвращать. Количество доступных полей зависит от выбранного типа графика.

      - В раскрывающемся списке слева выберите поля событий, данные по которым должны отображаться на виджете.

      - Среднее поле показывает, для чего выбранное поле используется в виджете: **metric** (метрики) или **value** (значение).

        > Если вы выбрали тип графика **Таблица**, в средних полях нужно указать названия столбцов, используя символы ANSII-ASCII.

      - В раскрывающемся списке справа вы можете выбрать операцию, которую следует произвести над данными:

        - **count** – подсчет событий. Эта операция доступна только для поля события **ID**. Используется по умолчанию для линейных, круговых и столбчатых диаграмм, а также для счетчиков. Является единственно возможным вариантом для календарных диаграмм.

        - **max** – максимальное значение поля **события** из выборки событий.

        - **min** – минимальное значение поля **события** из выборки событий.

        - **avg** – среднее значение поля **события** из выборки событий.

        - **sum** – сумма значений полей событий из выборки событий.

   b. **SOURCE** – тип источника данных. Для выбора доступно только значение **events** (события).

c. **WHERE** – условия фильтрации событий.

- В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.
- В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.
- В раскрывающемся списке справа введите значение условия. В зависимости от выбранного типа поля может потребоваться ввести значение вручную, выбрав его из раскрывающегося списка или в календаре.

Вы можете добавить условия поиска, нажав на кнопку **Добавить условие** или удалить их, нажав на кнопку ✕.

Вы можете добавить группы условий, нажав на кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **AND**, но при необходимости вы можете изменить значение. Доступные значения: **AND**, **OR**, **NOT**. Группы условий удаляются с помощью кнопки **Удалить группу**.

d. **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные. Этот параметр недоступен для графиков типа Счетчик.

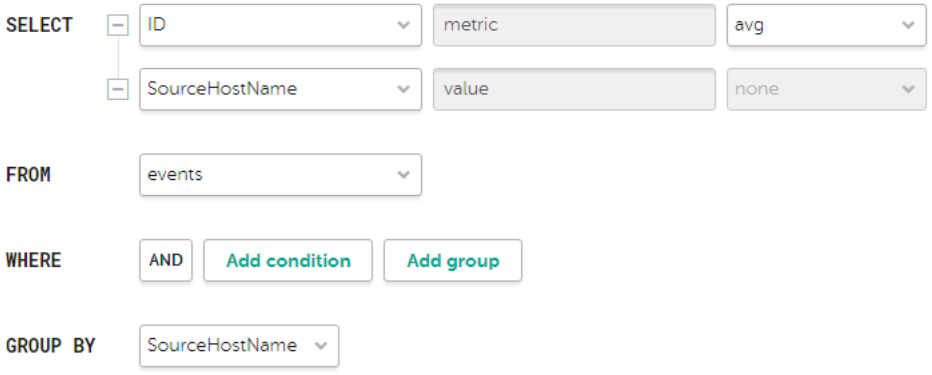
e. **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

- В раскрывающемся списке слева выберите значение, которое будет использоваться для сортировки.
- В раскрывающемся списке справа выберите порядок сортировки: **ASC** – по возрастанию, **DESC** – по убыванию.
- Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **Добавить столбец**.

f. **LIMIT** – максимальное количество точек данных для виджета. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

2. Нажмите **Применить**.

Пример условий поиска в конструкторе запросов



Параметры условий поиска для отображения в виджете среднего количества байт в расчете на один хост

Вкладка Оси

В таблице ниже описаны параметры, расположенные на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали одно из следующих значений: **Столбчатая диаграмма**, **Линейная диаграмма**, **Календарная диаграмма**.

Описание параметров

Параметр	Описание
Размер указателя	Размер указателя на графике. Поле отображается для типа графика **Линейная диаграмма**.
Толщина линии	Толщина линии на графике. Поле отображается для типа графика **Линейная диаграмма**.
Минимальное и максимальное значение для оси Y	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Минимальное и максимальное значение для оси X	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Вкладка Внешний вид

В таблице ниже описаны параметры, расположенные на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый;** • **красный;** • **синий;** • **желтый.** Параметр доступен для графиков типа **Столбчатая диаграмма**, **Счетчик**, **Линейная диаграмма**, **Календарная диаграмма**.
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа **Столбчатая диаграмма**, **Календарная диаграмма** (с видом диаграммы **Столбчатая диаграмма**), **Таблица**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.

Параметр	Описание
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
Итоговые значения	Суммы значений.
Длительность отрезков периода	Продолжительность сегментов, на которые вы хотите разделить период. Доступно для графика типа **Календарная диаграмма**.
Шкала	Шкала для отображения данных. Доступно для диаграммы типа **Сложенная столбчатая диаграмма**. Возможны следующие значения: • **Линейная** • **Квадратичная** • **Логарифмическая** По умолчанию выбрано значение **Линейная**.
Регрессия	Вариант указания среднего значения на графике. Возможны следующие значения: • **Не выбрано** • **Линейная** • **LOESS** (кривая с локально взвешенным сглаживанием диаграмм рассеяния) Доступно для графиков типа **Календарная диаграмма** и **Линейная диаграмма**.

Вкладка Действия

> Вкладка не отображается, если на вкладке **Общие** в поле График вы выбрали одно из следующих значений: **Счетчик**, **Спидометр**, **Таблица**.

На вкладке представлены параметры для настройки действий по нажатию левой кнопкой мыши на различных элементах виджетов, например, на сегменте графика или тексте элемента легенды. Вы можете выбрать следующие действия:

- Переход в события.
- Фильтрация по переменной.

  Параметры описаны в сценарии фильтрации данных на нескольких виджетах.
- Переход в другую панель мониторинга.

  Параметры описаны в сценарии перехода в другую панель мониторинга.

Виджет Активные листы

Вы можете использовать виджет **Активные листы** для получения аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Тип графика. Доступны следующие типы графиков: • **Столбчатая диаграмма** • **Круговая диаграмма** • **Счетчик** • **Таблица**

Параметр	Описание
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Коррелятор	Название коррелятора, содержащего активный лист, по которому вы хотите получать данные.
Активный лист	Название активного листа, по которому вы хотите получать данные. Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.
Поле SQL-запроса	В этом поле вы можете ввести запрос для фильтрации и поиска данных активного листа вручную. Структура запроса аналогична той, которая используется при поиске событий. При создании запроса по активным листам вам нужно учитывать следующие особенности: • Для функции FROM требуется указать значение `records`. • Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками: • в функции SELECT псевдонимы следует выделять двойными или косыми кавычками: "псевдоним", `другой псевдоним`; • в функции ORDER BY псевдонимы следует выделять косыми кавычками: `другой псевдоним`; • Значения полей событий выделяются прямыми кавычками: WHERE DeviceProduct = 'Microsoft'. • Название полей событий выделять кавычками не требуется. • Если название поля активного листа начинается или заканчивается пробелами, в виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов. • Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции LIKE '%значение поля%'. • Вы можете использовать в запросе служебные поля _key (поле с ключами записей активного листа) и _count (сколько раз эта запись была добавлена в активный лист), а также пользовательские поля. • Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по активным листам, кроме таблиц. • Если в SQL-запросе используется функция преобразования даты и времени (например, fromUnixTimestamp64Milli) и при этом обрабатываемое поле не содержит даты и времени, в виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250. • Если задать большие значения для функции LIMIT, это может привести к ошибкам в работе браузера. • Если в качестве типа графика вы выбрали Счетчик, необходимо для значений функции SELECT указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`. • В виджетах с графиком типа **Таблица** градиент строится по значениям поля, указанного в SQL-запросе (например, `_count`, `value`, `temp` или `name`). Это поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента** (если в запросе указано несколько числовых или временных полей, они все будут доступны для выбора). После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Если поле отсутствует в запросе, на вкладке **Внешний вид** не отображаются поля **Градиент** и **Поле с индикатором градиента**. Особенности использования псевдонимов в SQL-функциях: и SELECT допустимо использовать двойные и косые кавычки: ", `.  Если в качестве типа графика вы выбрали Счетчик, псевдонимы могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: "Псевдоним с пробелом", `Другой псевдоним`.  При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250.

Вы можете получать в виджете названия тенантов, а не их идентификаторы.

Если вы хотите, чтобы в виджетах по активным листам отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте. Процесс настройки состоит из следующих этапов:

1. Экспорт списка тенантов.

2. Создание словаря типа **Таблица** и импорт в него полученного ранее списка тенантов.

3. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

   Пример:

   - Переменная: `TenantName`.

   - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.

4. Добавьте действие с активными листами в правило корреляции. Это действие запишет значение ранее созданной переменной в формате "ключ-значение" в активный лист с помощью функции **Установить**. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** обратиться к ранее созданной переменной (например, `$TenantName`).

В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору среди словаря тенантов. При создании виджетов по активным листам можно получить название тенанта, обратившись к названию поля активного листа (в примере выше это `Тенант`).

Описанный метод можно применять и к другим полям событий с идентификаторами.

Примеры запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250`
  Запрос, который возвращает ключ активного листа с названием поля "Источник событий" и значением этого поля "Екатеринбург".
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация count по полю _key) и все варианты значений пользовательского поля Status. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля **Status**.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Запрос для таблицы, которая возвращает значения пользовательских полей **Name** и **Status**, а также служебного поля "_count" у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу ILIKE '%ftp%'. В виджете отображается таблица со столбцами **Status**, **Name** и **Number**.

Вкладка Оси

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали значение **Столбчатая диаграмма**.

Описание параметров

Settings	Описание
Минимальное значение Y и Максимальное значение Y	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Минимальное значение X и Максимальное значение X	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка Внешний вид

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый;** • **красный;** • **синий;** • **желтый.**
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа Столбчатая диаграмма, Таблица. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.

Виджет Контекстные таблицы

Вы можете использовать виджет **Контекстные таблицы** для получения аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для следующих параметров:

Вкладка :

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Доступны следующие типы графиков: • **Столбчатая диаграмма** • **Круговая диаграмма** • **Счетчик** • **Таблица**
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Коррелятор	Название коррелятора, содержащего контекстную таблицу, по которой вы хотите получать данные.
Контекстная таблица	Название контекстной таблицы, по которой вы хотите получать данные. Одна и та же контекстная таблица может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными корреляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.
Поле SQL-запроса	В этом поле вы можете ввести запрос для фильтрации и поиска данных контекстной таблицы вручную. По умолчанию для каждого типа графика в поле указан запрос, который получает схему контекстной таблицы и ключ по ключевым полям. Структура запроса аналогична той, которая используется при поиске событий. При создании запроса по контекстным таблицам вам нужно учитывать следующие особенности: • Для функции `FROM` требуется указать значение `` `records` ``. • Вы можете получить данных только по полям, указанным в схеме контекстной таблицы. • Вы можете использовать поддерживаемые функции ClickHouse. • Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками: • В функции `SELECT` псевдонимы следует выделять двойными или косыми кавычками: `"<псевдоним">`, `` `<другой псевдоним>` ``. • В функции `ORDER BY` псевдонимы следует выделять косыми кавычками: `` `<другой псевдоним>` ``. • Значения полей событий выделяются прямыми кавычками: `WHERE DeviceProduct = 'Microsoft'`. • Название полей событий выделять кавычками не требуется. • Если название поля активного листа начинается или заканчивается пробелами, в виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов. • Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции `LIKE '%< значение поля >%'`. • Вы можете использовать в запросе служебное поле `_count` (сколько раз эта запись была добавлена в контекстную таблицу), а также пользовательские поля. • Псевдонимы `metric` и `value` в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по активным листам, кроме таблиц. • Если в SQL-запросе используется функция преобразования даты и времени (например, `fromUnixTimestamp64Milli`) и при этом обрабатываемое поле не содержит даты и времени, в виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: `SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250`. • Если задать большие значения для функции `LIMIT`, это может привести к ошибкам в работе браузера. • Если в качестве типа графика вы выбрали **Счетчик**, необходимо для значений функции `SELECT` указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`. • В виджетах с графиком типа **Таблица** градиент доступен только для полей типа **INT**, **FLOAT** и для поля **_count**. Поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента**. После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Особенности использования псевдонимов в SQL-функциях и `SELECT`: допустимо использовать двойные и косые кавычки: ", `. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"<Псевдоним с пробелом>"`, Значения следует выделять прямыми одинарными кавычками: `'<Значение с пробелом>'`. При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру `metric`. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.

Вы можете получать в виджете названия тенантов, а не их идентификаторы.

Если вы хотите, чтобы в виджетах по активным листам отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте. Процесс настройки состоит из следующих этапов:

1. Экспорт списка тенантов.

2. Создание словаря типа **Таблица** и импорт в него полученного ранее списка тенантов.

3. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

   Пример:

   - Переменная: `TenantName`.

   - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.

4. Добавьте действие с активными листами в правило корреляции. Это действие запишет значение ранее созданной переменной в формате "ключ-значение" в активный лист с помощью функции **Установить**. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** обратиться к ранее созданной переменной (например, `$TenantName`).

В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору среди словаря тенантов. При создании виджетов по активным листам можно получить название тенанта, обратившись к названию поля активного листа (в примере выше это `Тенант`).

Описанный метод можно применять и к другим полям событий с идентификаторами.

Примеры запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250`
  Запрос, который возвращает ключ активного листа с названием поля "`Источник событий`" и значением этого поля "`Екатеринбург`".
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация `count` по полю **_key**) и все варианты значений пользовательского поля Status. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля **Status**.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Запрос для таблицы, которая возвращает значения пользовательских полей **Name** и **Status**, а также служебного поля **_count** у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу `ILIKE '%ftp%'`. В виджете отображается таблица со столбцами **Status**, **Name** и **Number**.

Вкладка :

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали значение **Столбчатая диаграмма**.

Описание параметров

Параметр	Описание
Ось Y и **Мин - Макс**	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Ось X и **Мин - Макс**	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка 🔧:

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Внешний вид**.

Описание параметров

Settings	Описание
Имя	Название виджета.
Описание	Описание виджета.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый;** • **красный;** • **синий;** • **желтый.**
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа **Столбчатая диаграмма**, **Таблицы**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.

Пользовательский виджет Активы

Вы можете использовать виджет **Активы** → **Пользовательский виджет** для получения расширенной аналитики по активам из обработанных событий с помощью конструктора запросов. В запросе необходимо указать поле актива и соответствующее ему условие или набор условий, по которым должен вестись подсчет активов (ось Y). Также вы можете указать одно или несколько дополнительных условий (категорий), по которым будет производиться сравнение количества активов для каждого поля.

При создании пользовательского виджета активов вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, расположенные на вкладке **Общие**.

Описание параметров

Параметр	Описание
Название	Название виджета. При сохранении отчета в формате Excel название виджета, отображаемое в заголовке листа, ограничено 31 символом. Рекомендуется называть виджеты с учетом этого ограничения.
График	Тип графика. Доступны следующие типы графиков: • **Круговая диаграмма**. Отображается распределение активов по указанным категориям для всех выбранных тенантов. • **Счетчик**. Подсчет активов выполняется только по одному условию. На диаграмме отображается сумма активов, соответствующих условию, по всем выбранным тенантам. • **Таблица**. Подсчет активов выполняется по указанным категориям по всем выбранным тенантам. Каждой категории на диаграмме соответствует отдельная строка. Название категории отображается в столбце **value**. Количество активов, соответствующих условию, отображается в столбце **metric**. • **Столбчатая диаграмма с накоплением**. Подсчет активов выполняется по указанным категориям по всем выбранным тенантам с возможностью группировки по тенантам (в этом случае отдельные тенанты располагаются по оси X). Каждой категории соответствует своя область на столбцах диаграммы, выделенная отдельным цветом. Названия категорий отображаются в легенде. С помощью флажков слева от названий категорий можно скрыть или показать соответствующие области на столбцах. • **Спидометр**. Подсчет активов выполняет с помощью соотношения количества активов, удовлетворяющих указанному условию, и общего количества активов. Значения на графике указываются в процентах.
Формат	Параметр доступен для графика типа **Столбчатая диаграмма с накоплением**. Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Категория активов	Категория активов, для которой отображаются данные на виджете.
Искать в активах без категории	Параметр позволяет отображать активы без категории. По умолчанию флажок не установлен.
Группа параметров **Выбор осей графика**	
Ось Y	Обязательный параметр. Поле актива и указанное для этого поля условие или набор условий, по которым должен вестись подсчет активов.
Категория оси Y	Категория для выбранного поля. Не используется для графика типа **Счетчик**. Параметр является необязательным для полей оси Y, значения которых являются перечислением (могут выбираться из конечного списка значений). Для всех остальных полей параметр является обязательным.
Группировка по тенантам	Параметр доступен для графика типа **Столбчатая диаграмма с накоплением**. Задает дополнительную группировку активов по тенантам. Если флажок установлен, активы на диаграмме разбиваются по оси X на столбцы, соответствующие отдельным тенантам. Если флажок не установлен, все активы отображаются на одном столбце. По умолчанию флажок не установлен.

Вкладка Внешний вид.

В таблице ниже описаны параметры, расположенные на вкладке **Внешний вид**.

Параметр	Описание
Описание	Описание виджета.
Итоговые значения	Параметр доступен для графика типа **Круговая диаграмма**. Включает отображение итоговых значений на диаграмме, помимо выбранных категорий. Если переключатель включен, сумма значений всех указанных категорий отображается в центре круговой диаграммы и в легенде в отдельной графе **Всего**. По умолчанию переключатель выключен.
Цвет	Параметр доступен для графика типа **Счетчик**. Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Параметр доступен для графика типа **Таблица**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором будут отображаться маркеры градиентной заливки. Этот столбец определяется полем **Metric**, выбранном в раскрывающемся списке. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Отображать проценты в легенде	Отображение процентных значений в легенде. По умолчанию переключатель включен.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.
Шкала	Доступно для графика типа **Столбчатая диаграмма с накоплением**. Шкала для отображения данных. Возможны следующие значения: • **Линейная**. • **Квадратичная**. • **Логарифмическая**. По умолчанию выбрано значение **Линейная**.
Пороговые значения	Доступно для графика типа **Спидометр**. По умолчанию установлены следующие интервалы значений: 0–30, 30–70, 70–100.

Другие виджеты

В этом разделе описываются параметры всех виджетов, кроме виджетов **События**, Активные листы, Контекстные таблицы и пользовательский виджет **Активы**.

Набор параметров, доступных для виджета, зависит от типа графика, который отображается на виджете. В KUMA доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).

- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.

Параметры для круговых диаграмм

В таблице ниже представлены параметры для графиков типа **Круговая диаграмма**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для счетчиков

В таблице ниже представлены параметры для графиков типа **Счетчик**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.

Параметры для таблиц

В таблице ниже представлены параметры для графиков типа **Таблица**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Этот столбец определяется полем, выбранным в раскрывающемся списке. Тип поля зависит от типа виджета: • **Затронутые активы** – поле **Frequency**. • **Активы в инцидентах**, **Расширенный статус постоянной защиты активов из KSC**, **Пользователи в инцидентах** – поле **Count**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для столбчатых и календарных диаграмм

В таблице ниже представлены параметры для графиков типа **Столбчатая диаграмма** и **Календарная диаграмма**, расположенные на вкладке **Оси**.

Описание параметров

Параметр	Описание
Ось Y и **Мин - Макс**	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Ось X и **Мин - Макс**	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

В таблице ниже представлены параметры для графиков типа **Столбчатая диаграмма**, **Сложенная столбчатая диаграмма** и **Календарная диаграмма**, расположенные на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Формат	Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. Параметр доступен для графика типа **Сложенная столбчатая диаграмма**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Вид временной диаграммы	Формат отображения временных данных: **Столбчатая диаграмма** или **Линейная диаграмма**. Параметр доступен для графика типа **Календарная диаграмма**. При выборе формата **Столбчатая диаграмма** данные по умолчанию отображаются в виде вертикальных столбцов. Если SQL-запрос содержит дополнительное поле с псевдонимом category, столбчатая диаграмма будет представлена в виде сложенной диаграммы, то есть с разбивкой каждого столбца по значениям этого поля. При выборе формата **Линейная диаграмма** данные отображаются в виде одной или нескольких (в зависимости от запроса) ломаных линий, соединяющих точки на временной оси. По умолчанию выбран формат Столбчатая диаграмма.
Показывать данные за предыдущий период	Включение отображения данных сразу за два периода: текущий и предыдущий.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**.
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней. Градиентная заливка не применяется для сложенных столбчатых диаграмм. В этом случае цвета назначаются автоматически.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Длительность отрезков периода	Продолжительность сегментов, на которые вы хотите разделить период. Доступно для графиков типа **Календарная диаграмма**.

Параметры для графиков типа Спидометр

В таблице ниже представлены параметры для графика **Спидометр**.

> Значения на графике указываются в процентах.

Описание параметров

Параметр	Описание
Вкладка **Общие**	
Имя	Название виджета.
Тенант	Тенант, данные которого отображаются на виджете. Можно выбрать только те тенанты, которые вы выбрали ранее в параметрах панели мониторинга.
Категория активов	Активы выбранной категории, по которым будет осуществляться поиск значений.
Искать в активах без категории	Поиск активов для формирования графика осуществляется без учета категорий активов.
Ось Y	Указывается значение параметра, по которому будет выполнятся поиск активов и дальнейшее вычисление показания спидометра. Вы можете указать несколько значений параметров для поиска активов.
Вкладка **Внешний вид**	
Описание	Описание графика, которое отображается на виджете.
Предел событий	Для визуального определения критичности события циферблат спидометра разделен на три области: зеленую, желтую и красную. По умолчанию для этих областей определены следующие интервалы: • зеленый: 0–30; • желтый: 30–70; • красный: 70–100. При необходимости вы можете изменить интервалы значений.

Настройка значения периода

Для таких графиков, как **Круговая диаграмма**, **Счетчик**, **Таблица**, **Столбчатая диаграмма**, **Сложенная столбчатая диаграмма**, **Календарная диаграмма**, вы можете настроить период отображения данных в виджете с помощью параметра **Период**. По умолчанию период отображения данных виджета совпадает с периодом отображения данных панели мониторинга.

Чтобы настроить период отображения данных, выполните одно из следующих действий:

- При необходимости измените дату и время в параметре **Период** одним из следующих способов:

  - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

    Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

  - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

    Период рассчитывается относительно настоящего времени.

- Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

  Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

  В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

  > Поле **Дата от** является обязательным, и его значение не может превышать значение, установленное в поле **Дата до**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **Дата до**, параметр **now** указывается автоматически.

Время в KUMA хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

Границы периода включаются: например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 UTC до 00:00:00:000 UTC сегодняшнего дня. Вы можете посмотреть дату и время последнего обновления данных и точный период, за который отображаются данные, наведя курсор на значок периода на виджете.

Если параметр Показать данные за предыдущий период включен в свойствах виджета и виджет отображает данные за относительный период, во всплывающей подсказке также отображается предыдущий период. Предыдущий период рассчитывается относительно текущего периода – из начального и конечного значения текущего периода вычитается продолжительности текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

- Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Фильтрация данных на виджетах

KUMA позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга. Вы можете применять фильтрацию данных в следующих случаях:

- Фильтрация данных на одном виджете

  Для фильтрации данного типа вам нужно прописать одну или несколько локальных переменных в SQL-запросе в свойствах виджета. Переменные позволяют вам изменять этот SQL-запрос, подставляя в него данные, которые представлены на виджете в панели мониторинга. Виджет отфильтрует данные с учетом новых значений переменных и перестроит график. При этом вам не нужно вручную изменять SQL-запрос в свойствах виджета.

  Локальные переменные вы можете применить, нажав на значок воронки (▽) на виджете. В открывшемся окне вы сможете выбрать или ввести значения для локальных переменных.

- Фильтрация данных на нескольких виджетах в рамках одной панели мониторинга

  Для фильтрации данного типа вам нужно прописать одну или несколько глобальных переменных в свойствах панели мониторинга. Затем добавьте глобальные переменные в SQL-запросы виджетов, к которым хотите применять эти глобальные переменные. Когда вы присваиваете глобальной переменной новое значение, все виджеты, в которых эта переменная используется, автоматически перестраивают графики с учетом нового значения.

  Для применения глобальных переменных нужно нажать на сегмент графика или на текст из легенды графика. KUMA отобразит меню с командами, позволяющими применить категорию данных выбранного сегмента графика или значение элемента легенды графика к переменной.

- Переход в другую панель мониторинга с одновременной передачей параметров фильтрации

  Глобальные переменные можно использовать для передачи значений в другую панель мониторинга. При переходе из одной панели мониторинга в другую KUMA подставит выбранное значение переменной и выбранный временной период, а графики в новой панели автоматически перестроятся.

  Локальные переменные не могут быть использованы при переходе в другую панель мониторинга.

Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Фильтрация данных на одном виджете

KUMA позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга.

Для фильтрации данных на одном виджете вам нужно прописать одну или несколько локальных переменных в SQL-запросе в свойствах виджета. Переменные позволяют вам изменять этот SQL-запрос, подставляя в него данные, которые представлены на виджете в панели мониторинга. Виджет отфильтрует данные с учетом новых значений переменных и перестроит график. При этом вам не нужно вручную изменять SQL-запрос в свойствах виджета.

Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Настройка фильтрации данных на одном виджете

Чтобы настроить локальные переменные для фильтрации данных в рамках одного виджета:

1. В разделе **Панели мониторинга** выберите панель мониторинга и затем нажмите на кнопку **Изменить**, чтобы перейти в режим редактирования панели мониторинга.

2. Выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

3. В окне свойств виджета перейдите на вкладку **Общие**.

4. В блоке параметров **Доступные переменные** нажмите на кнопку **Добавить**.

5. Введите произвольное имя переменной, затем укажите значение переменной. Имена локальных и глобальных переменных должны быть уникальными в рамках панели мониторинга.

   В качестве значения переменной укажите `value` или `category`, то есть псевдонимы полей, используемые в запросе. Если хотите при фильтрации данных в виджете вводить значение этой переменной вручную, оставьте поле пустым.

   Для графиков типа таблица в качестве значения переменной вы можете указать название поля события. Тогда вы сможете фильтровать данные в таблице по выбранному значению этого поля. Название поля события будет отображаться в заголовке столбца таблицы.

6. В поле **SQL-запрос** в оператор WHERE добавьте функцию для работы с переменными.

   Синтаксис для переменных с конкретным значением:

   `filter(< название_поля_события > = $ имя_переменной )`

   Синтаксис для переменных с произвольным значением, которое задается вводом вручную:

   `filter(< название_поля_события > like $ имя_переменной )`

   В этом случае при вводе вручную вы можете использовать метасимвол % для поиска частичных текстовых совпадений. Подробную информацию смотрите в документации ClickHouse.

   > Вы не можете использовать конструктор SQL для добавления переменных в SQL-запрос.

   Посмотреть пример

   Пример SQL-запроса с использованием локальной переменной

   ```
   SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name)
   GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250
   ```

   В этом запросе использована локальная переменная `$Name`. В эту переменную будет подставляться значение из поля события `Name`. Вы можете применить переменную, нажав на значок воронки (▽) на виджете. В открывшемся окне вы сможете выбрать значение для переменной. Виджет отфильтрует выборку по выбранному значению поля `Name`.

   Обратите внимание, если в SQL-запросе вы указываете переменную для поля, которое принимает числовое значение, такое значение надо преобразовать в строку. Для этого используйте функцию `toString`. Иначе SQL-запрос вернет ошибку.

   Пример

   ```
   SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like
   $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250
   ```

В этом запросе поле события `SourcePort` имеет числовое значение, поэтому оно преобразовано в строку `toString(SourcePort)`.

7. Сохраните изменения.

Применение фильтрации данных на одном виджете

Чтобы применить локальную переменную для фильтрации данных в рамках одного виджета:

1. В разделе **Панели мониторинга** выберите панель мониторинга, на которой расположен требуемый виджет. В свойствах этого виджета должна быть задана хотя бы одна локальная переменная.

2. На виджете нажмите на значок воронки ( ).

3. В открывшемся окне выберите, какие локальные переменные вы хотите применить.

4. Сохраните изменения.

   Виджет перестроит график с учетом нового значения переменной.

Фильтрация данных на нескольких виджетах

KUMA позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга.

Для фильтрации данных на нескольких виджетах в рамках одной панели мониторинга вам нужно прописать одну или несколько глобальных переменных в свойствах панели мониторинга. Затем добавьте глобальные переменные в SQL-запросы виджетов, к которым хотите применять эти глобальные переменные. Когда вы присваиваете глобальной переменной новое значение, все виджеты, в которых эта переменная используется, автоматически перестраивают графики с учетом нового значения.

Глобальные переменные применяются по щелчку кнопкой мыши на сегменте графика или на тексте из легенды графика. KUMA отобразит меню с командами, позволяющими применить категорию данных выбранного сегмента графика или значение элемента легенды графика к переменной.

> Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Настройка фильтрации данных на нескольких виджетах на уровне панели мониторинга

Чтобы настроить глобальные переменные для фильтрации данных на уровне панели мониторинга:

1. В разделе **Панели мониторинга** выберите панель мониторинга и затем нажмите на кнопку **Изменить**, чтобы перейти в режим редактирования панели мониторинга.

2. Нажмите на кнопку **Настройки**.

3. В открывшемся окне в разделе **Переменные** перейдите на вкладку **Глобальные переменные**.

4. Нажмите на кнопку **Добавить**.

5. В добавленную строку введите имя переменной. Имена локальных и глобальных переменных должны быть уникальными в рамках панели мониторинга.

   Названия всех виджетов панели мониторинга, в которые вы добавите глобальные переменные, будут перечислены в столбце **Используется в виджетах**.

Имена глобальных переменных будет отображаться в командах контекстного меню виджета по щелчку на сегменте графика или на элементе легенды графика.

6. Сохраните изменения.

7. Выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**. В этом виджете настройте действия по нажатию на кнопку мыши.

8. В окне свойств виджета перейдите на вкладку **Общие**.

9. В разделе **Доступные переменные** добавьте одну или несколько глобальных переменных, которые вы добавили в свойствах панели мониторинга.

10. Если необходимо, в поле SQL-запроса добавьте глобальные переменные в оператор WHERE с помощью функции filter. В этом случае настраиваемые действия будут также применяться и к этому виджету.

11. Перейдите на вкладку **Действия**.

    Если вы хотите, чтобы при щелчке на сегменте графика отображалось меню с командой для фильтрации данных по выбранной категории сегмента:

    a. В разделе **Сегмент графика** включите параметр **Фильтровать по переменной**.

    b. В списке **Категория** выберите переменную, в которую вы хотите иметь возможность подставлять значение псевдонима `category`, указанного в SQL-запросе.

       Параметр **Категория** доступен только для типа графика сложенная столбчатая диаграмма.

    c. В списке **Значение** выберите переменную, в которую вы хотите иметь возможность подставлять значение псевдонима `value`, указанного в SQL-запросе.

    Если вы хотите, чтобы при щелчке на элементе легенды графика отображалось меню с командой для фильтрации данных по выбранному значению:

    a. В разделе **Элемент легенды** включите параметр **Фильтровать по переменной**.

       При необходимости нажмите на кнопку **Скопировать из параметров сегмента графика**, чтобы автоматически перенести выбранные значения параметров из блока параметров **Сегмент графика** в блок параметров **Элемент легенды**.

    b. В списке **Значение** выберите переменные, в которые вы хотите иметь возможность подставлять значение элемента легенды.

12. В свойствах других виджетов, к которым вы хотите применять глобальные переменные:

    - На вкладке **Общие** в разделе **Доступные переменные** добавьте одну или несколько глобальных переменных.

    - В поле SQL-запроса виджета добавьте глобальные переменные в оператор WHERE с помощью функции filter.

Применение фильтрации данных на нескольких виджетах на уровне панели мониторинга

Чтобы применить глобальную переменную для фильтрации данных между виджетами:

1. В разделе **Панели мониторинга** выберите панель мониторинга, к виджетам которой хотите применить глобальную переменную.

2. Найдите виджет, в свойствах которого прописаны действия по щелчку кнопкой мыши. Щелкните на сегменте графика или на значке стрелки (⌄) рядом с элементом легенды графика, чтобы открыть меню.

3. В меню нажмите **Применить категорию к переменной <имя переменной>** или **Применить значение к переменной <имя переменной>**.

   Переменная примет значение выбранной категории или выбранного элемента легенды. В рамках текущей панели мониторинга все виджеты, в которых используется эта переменная, перестроят графики с учетом нового значения переменной. Такие виджеты будут помечены значком воронки с цифрой, обозначающей количество примененных фильтров (1). В верхней части экрана появится список примененных глобальных переменных. Чтобы отменить фильтрацию данных для виджета, нажмите на значок воронки с цифрой (1). Чтобы отменить фильтрацию данных для всех виджетов панели мониторинга, нажмите **Сбросить все** в верхней части панели мониторинга.

Переход в связанную панель мониторинга

KUMA позволяет фильтровать данные на виджетах типа **События** в текущей панели мониторинга и переходить на другую панель мониторинга с сохранением настроенных параметров фильтрации и периода.

Для этого используются глобальные переменные. Они должны быть настроены в обеих панелях мониторинга, а также в свойствах виджетов: на целевой панели переменная указывается в SQL-запросе, а на исходной панели указывается при настройке параметра **Переход к другой панели мониторинга**. При переходе из одной панели мониторинга в другую KUMA автоматически подставляет выбранное значение переменной и период, после чего графики в целевой панели перестраиваются. Обе панели должны находиться в одном тенанте.

Локальные переменные не могут использоваться при переходе в другую панель мониторинга.

Настройка целевой панели мониторинга

Чтобы настроить целевую панель мониторинга:

1. В веб-интерфейсе KUMA в разделе **Панели мониторинга** выберите панель мониторинга и создайте глобальную переменную.

   Имя переменной должно содержать только английские буквы, цифры и не должно содержать пробелы.

2. Сохраните изменения.

3. В панели мониторинга выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

4. На вкладке **Общие** укажите созданную ранее переменную:

   - В блоке параметров **Доступные переменные**.

   - В поле **SQL-запрос**. Для того чтобы SQL-запрос учитывал значение переменной, добавьте в условие `WHERE` функцию `filter()`.

     Синтаксис для переменных с конкретным значением:

     `filter(<название_поля_события> = $имя_переменной)`

Синтаксис для переменных с произвольным значением, которое задается вручную:

`filter(< название_поля_события > like $ имя_переменной )`

Пример запроса

Запрос с переменной `$ServiceName`:

```
SELECT DestinationHostName AS Host, Name AS Status, Message AS Reason, ServiceName,
Timestamp AS Time
FROM events
WHERE DeviceEventClassID = 'KLSRV_HOST_STATUS_CRITICAL' OR DeviceEventClassID =
'KLSRV_HOST_STATUS_WARNING' AND filter(ServiceName = $ServiceName)
ORDER BY Time DESC
LIMIT 25
```

Если при переходе в целевую панель мониторинга переменной `$ServiceName` передается значение, оно автоматически подставляется в запрос и данные фильтруются. Если значение переменной не задано, запрос выполняется так, как будто переменной в нем нет.

5. Сохраните изменения.

Настройка исходной панели мониторинга

Чтобы настроить исходную панель мониторинга:

1. В веб-интерфейсе KUMA в разделе **Панели мониторинга** выберите панель мониторинга и создайте глобальную переменную.

   Имя переменной должно совпадать с именем переменной, созданной на целевой панели. Имя должно содержать только английские буквы, цифры и не должно содержать пробелы.

2. Сохраните изменения.

3. В панели мониторинга выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

4. На вкладке **Общие** в блоке параметров **Доступные переменные** укажите созданную ранее переменную.

5. На вкладке **Действия** настройте следующие параметры:

   a. В разделе **Сегмент графика** или **Элемент легенды** включите параметр **Переход к другой панели мониторинга**.

   b. В раскрывающемся списке **Панели мониторинга** выберите целевую панель.

   c. В раскрывающемся списке **Значение** выберите переменную, значение которой будет передаваться при переходе. Это должна быть та же переменная, которую вы создали ранее.

      Выбранная переменная должна быть указана в SQL-запросе виджета целевой панели, чтобы данные на этом виджете автоматически были отфильтрованы после перехода.

6. Сохраните изменения.

Переход из исходной панели мониторинга в целевую панель мониторинга

Чтобы перейти в целевую панель мониторинга:

1. В веб-интерфейсе KUMA в разделе **Панели мониторинга** выберите исходную панель мониторинга.

2. Найдите виджет, в свойствах которого вы включили параметр **Переход к другой панели мониторинга**. Нажмите на сегмент или элемент легенды графика, для которых задано это действие.

   В новой вкладке откроется целевая панель мониторинга. При этом автоматически ко всей панели применится период исходного виджета, а выбранное значение в раскрывающемся списке **Значение** передастся как переменная в виджеты типа **События**, где эта переменная используется в SQL-запросе через функцию `filter()`. Графики в виджетах на другой панели перестроятся с учетом полученных параметров.

   > Если на целевой панели мониторинга, в которую выполняется переход, изменили или удалили переменную, которая указана в действии, переход будет выполняться, но значение переменной передаваться не будет.

Отображение названий тенантов в виджетах типа Активный лист

Если вы хотите, чтобы в виджетах типа **Активные листы** отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте.

Процесс настройки состоит из следующих этапов:

1. Экспорт списка тенантов.

2. Создание словаря типа **Таблица**.

3. Импорт списка тенантов, полученного на шаге 1, в словарь, созданный на шаге 2 этой инструкции.

4. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

   Пример:

   - Переменная: `TenantName`.

   - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.

5. Добавление в корреляционное правило действия **Установить**, с помощью которого значение ранее созданной переменной будет записываться в активный лист в формате <ключ> – <значение>. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** указать переменную (например, `$TenantName`).

В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору в словаре тенантов. При создании виджетов по активным листам в виджете вместо идентификатора тенанта будет отображаться название тенанта.

Информационная панель Обнаружение и реагирование

В разделе **Панель мониторинга** вы можете контролировать состояние безопасности сети вашей организации.

Панель мониторинга представляет собой набор виджетов, которые отображают аналитику данных безопасности сети. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

Набор виджетов, используемых в панели мониторинга, называется *макетом*. Вы можете создавать макеты вручную или воспользоваться преднастроенными макетами. Параметры виджетов в преднастроенных макетах можно редактировать при необходимости. По умолчанию в панели мониторинга отображается преднастроенный макет Alerts Overview.

Создавать, редактировать и удалять макеты могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик 2-го уровня и Аналитик 1-го уровня. Пользователи с учетными записями всех ролей могут просматривать макеты и назначать макеты по умолчанию. Если макет назначен по умолчанию, этот макет отображается для учетной записи при каждом переходе в раздел **Панель мониторинга**. Выбранный макет по умолчанию сохраняется для текущей учетной записи пользователя.

Информация в панели мониторинга обновляется в соответствии с расписанием, заданным в параметрах макета. При необходимости вы можете обновить данные принудительно.

Для удобства представления данных в панели мониторинга вы можете включить режим ТВ. В этом случае вы перейдете в режим полноэкранного просмотра панели мониторинга в FullHD-разрешении. В режиме ТВ вы также можете настроить отображение слайд-шоу для выбранных макетов.

Создание макета панели мониторинга

Чтобы создать макет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Откройте раскрывающийся список в правом верхнем углу окна и выберите **Создать макет**.

   Откроется окно **Новый макет**.

3. В раскрывающемся списке **Тенанты** выберите тенанты, которым будет принадлежать созданный макет и данные которых будут использоваться для заполнения виджетов макета.

   Выбор тенантов в этом раскрывающемся списке не имеет значения, если вы хотите создать универсальный макет (шаг 8).

4. В раскрывающемся списке **Период** выберите период, за который требуется аналитика:

   - **1 час**
   - **1 день** (это значение выбрано по умолчанию)
   - **7 дней**
   - **30 дней**

- **За период** – получать аналитику за выбранный период. Период устанавливается с помощью календаря, который отображается при выборе этого параметра.

  > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите как часто нужно обновлять данные в виджетах макета:

   - **1 минута**
   - **5 минут**
   - **15 минут**
   - **1 час** (это значение выбрано по умолчанию)
   - **24 часа**

6. В раскрывающемся списке **Добавить виджет** выберите нужный виджет и настройте его параметры.

   В макет можно добавить несколько виджетов.

   Вы также можете перетаскивать виджеты по окну и изменять их размер с помощью диагональной кнопки (⤡), которая появляется при наведении курсора мыши на виджет.

   Вы можете изменять или удалять виджеты, добавленные на макет. Для этого нажмите на значок параметров (⚙) и выберите пункт **Изменить**, чтобы изменить их конфигурацию, или пункт **Удалить**, чтобы удалить их из макета.

7. В поле **Имя макета** введите уникальное имя для этого макета. Имя должно содержать от 1 до 128 символов Юникода.

   Пользовательские панели мониторинга не могут иметь названия предустановленных панелей мониторинга.

   При попытке создать панель мониторинга с тем же именем, что и стандартная панель мониторинга, или сменить имя пользовательской панели мониторинга на имя предопределенной панели мониторинга в тенанте Main. В тенантах кроме Main нет ограничений по копированию или дублированию пользовательской панели мониторинга с тем же именем, что и у предопределенной панели мониторинга.

8. При необходимости нажмите на значок параметров (⚙) справа от поля названия макета и установите флажок рядом с параметром **Универсальные**.

   Виджеты макета будут отображать данные тенантов, которые вы выбрали в разделе **Выбранные тенанты** в меню слева. Это означает, что данные в виджетах макета будут изменяться в зависимости от выбранных вами тенантов без необходимости изменять параметры макета. Для универсальных макетов **тенанты**, выбранные в раскрывающемся списке, не учитываются.

   Если флажок снят, виджеты макета отображают данные от тенантов, выбранных в раскрывающемся списке **Тенанты** в параметрах макета. Если какой-либо из выбранных в макете тенантов недоступен для вас, их данные не будут отображаться в виджетах макета.

Вы не можете использовать виджет **Активные листы** в универсальных макетах.
Универсальные макеты может создавать и изменять только пользователь, которому назначена роль Главного администратора. Такие макеты могут просматривать все пользователи.

9. Нажмите на кнопку **Сохранить**.

Макет будет создан и отобразится на вкладке **Обнаружение и реагирования** в панели мониторинга.

Выбор макета панели мониторинга

Чтобы выбрать макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Выберите соответствующий макет.

Выбранный макет отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Выбор макета панели мониторинга по умолчанию

Чтобы установить макет в панели мониторинга по умолчанию:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок звездочка (☆).

Выбранный макет по умолчанию отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Изменение макета панели мониторинга

Чтобы изменить макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок редактирования ( ).

   Откроется окно **Настройка макета**.

5. Измените макет панели мониторинга. Параметры, доступные для изменения, такие же, как и параметры, доступные при создании макета.

6. Нажмите на кнопку **Сохранить**.

Макет панели мониторинга изменен и отображается на вкладке **Обнаружение и реагирование**.

Если макет был удален или назначен другому тенанту во время его изменения, при нажатии на кнопку **Сохранить** отображается ошибка. Макет не сохранен. Обновите страницу интерфейса Kaspersky EDR Expert, чтобы увидеть список доступных макетов в раскрывающемся списке.

Удаление макета панели мониторинга

Чтобы удалить макет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Раскройте список в правом верхнем углу окна.

3. Наведите курсор мыши на соответствующий макет.

4. Нажмите на значок удаления (🗑) и подтвердите это действие.

Макет удален.

Включение и отключение режима ТВ

Мы рекомендуем для отображения аналитики в режиме ТВ создать отдельного пользователя с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.

2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.

3. Переведите переключатель **Режим ТВ** в положение **Включено**.

4. Чтобы настроить показ виджетов в режиме слайд-шоу:

   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.

   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение макетов.

   c. В раскрывающемся списке **Очередь** выберите виджеты для просмотра. Если макет не выбран, в режиме слайд-шоу по очереди отображаются все доступные пользователю макеты.

   d. Если требуется, измените порядок показа макетов, перетащив их с помощью кнопки ⣿.

5. Нажмите на кнопку **Сохранить**.

Режим ТВ включен. Чтобы вернуться к работе с Консолью KUMA, нужно выключить режим ТВ.

Чтобы отключить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Выключено**.
4. Нажмите на кнопку **Сохранить**.

Режим ТВ выключен. В левой части экрана отобразится панель с разделами Консоли KUMA.

Когда вы вносите изменения в макеты, выбранные для слайд-шоу, эти изменения будут автоматически применены к активным сеансам слайд-шоу.

Преднастроенные макеты панели мониторинга

Kaspersky EDR Expert поставляется с набором преднастроенных макетов, которые содержат следующие виджеты:

- Макет **Alerts Overview** (Обзор алертов):
  - Active alerts (Активные алерты) – количество незакрытых алертов.
  - Неназначенные алерты – количество алертов, у которых нет исполнителя.
  - Latest alerts (Последние алерты) – таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в макете тенантам.
  - Alerts distribution (Распределение алертов) – количество алертов, созданных в течение указанного для виджета периода.
  - Alerts by priority (Алерты по приоритету) – количество незакрытых алертов, сгруппированных по приоритету.
  - Alerts by users (Алерты по пользователям) – количество алертов со статусом **В обработке**. Сгруппированы по имени учетной записи.
  - Alerts by status (Алерты по статусам) – количество алертов, сгруппированных по статусу.
  - Alerts by groups (Алерты по группам) – количество алертов, сгруппированных по группам пользователей.
  - Affected users in alerts (Пользователи в алертах) – пользователи, связанные с незакрытыми алертами.
  - Affected assets (Затронутые активы) – таблица с информацией об активах, их уровне важности и количестве связанных с ними незакрытых алертов. Уровень важности актива рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.
  - Категории затронутых активов – диаграмма, на которой отображено количество категорий активов, указанных в незакрытых алертах и инцидентах. Для каждого актива, указанного в алертах и инцидентах, уровень важности рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.

- Топ источников событий по количеству алертов – количество незакрытых алертов, сгруппированных по источникам событий, который сгенерированы алертами.

  На виджете отображается не более 10 источников событий.

- Alerts by rule (Алертов по правилу) – количество незакрытых алертов, сгруппированных по правилам корреляции.

Незакрытые алерты – это алерты, которые имеют один из следующих статусов: **Новый**, **В обработке**, **В инциденте**.

- Макет **Incidents Overview** (Обзор инцидентов):

  - Active incidents (Активные инциденты) – количество инцидентов, статусы которых отличны от **Завершен**.
  - Unassigned Incidents (Неназначенные инциденты) – количество инцидентов, у которых нет исполнителя.
  - Latest Incidents (Последние инциденты) – таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.
  - Incidents distribution (Распределение инцидентов) – количество инцидентов, созданных в течение указанного для виджета периода.
  - Incidents by priority (Инциденты по приоритету) – количество незакрытых инцидентов, сгруппированных по приоритету.
  - Incidents by users (Инциденты по пользователям) – количество инцидентов со статусом **В обработке**. Сгруппированы по имени учетной записи пользователя.
  - Incidents by status (Инциденты по статусам) – количество инцидентов, сгруппированных по статусу.
  - Incidents by groups (Инциденты по группам) – количество незакрытых инцидентов, сгруппированных по группам пользователей.
  - Affected assets in incidents (Активы в инцидентах) – таблица с количеством активов, связанных с незакрытыми инцидентами. В таблице перечислены активы и их уровень важности – он рассчитывается на основе категорий, к которым принадлежит актив, вместе со всеми родительскими категориями до корня иерархии.
  - Affected users in incidents (Пользователи в инцидентах) – пользователи, связанные с незакрытыми инцидентами.
  - Affected asset categories in incidents (Категории затронутых активов в инцидентах) – график с количеством категорий активов, связанных с незакрытыми инцидентами. Для каждого актива, связанного с инцидентом, уровень важности рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.
  - Active incidents by tenant (Инциденты по тенантам) – количество незакрытых инцидентов, сгруппированных по тенантам.

Незакрытые инциденты – это инциденты, статусы которых отличны от **Завершен**.

- Макет **Network Overview** (Обзор сетевой активности):
  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внутренним IP-адресам активов.

    На виджете отображается не более 10 IP-адресов.
  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внешним IP-адресам активов.
  - Netflow top hosts for remote control (Топ активов, на которые были обращения на порты для удаленного управления) – количество событий, связанных с обращением на один из следующих портов: 3389, 22, 135. Данные сгруппированы по именам активов.
  - Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика) – количество байт, переданное на внутренние порты активов. Данные сгруппированы по номерам портов.
  - Top Log Sources by Events count (Топ источников событий) – 10 источников, от которых было получено наибольшее количество событий.
- Макет **Агрегированные панели мониторинга NGFW**:
  - NGFW. Firewall Sessions & Actions (Сессии и действия сетевого экрана) – количество примененных действий разного типа в правилах фильтрации, для которых включено ведение журнала.
  - NGFW. DNS Security Sessions & Actions (Сессии и действия Защиты DNS-трафика) – количество примененных действий разного типа в профилях Защиты DNS-трафика, для которых включено ведение журнала.
  - NGFW. Web Control Sessions & Actions (Сессии и действия Веб-Контроля) – количество примененных действий разного типа в профилях Веб-Контроля, для которых включено ведение журнала.
  - NGFW. IDPS Sessions & Actions (Сессии и действия IDPS) – количество примененных действий разного типа в профилях IDPS, для которых включено ведение журнала.
  - NGFW. Anti-Virus Sessions & Actions (Сессии и действия Антивируса) – количество примененных действий разного типа в профилях Антивируса, для которых включено ведение журнала.
- Макет **NGFW IDPS & File Web Antivirus**:
  - NGFW. IDPS. Top-5 Threats Name (Топ 5 названий угроз) – пять угроз, чаще всего обнаруженных профилями IDPS.
  - NGFW. IDPS. Top-5 MITRE Tactics & Techniques (Топ 5 тактик и техник MITRE) – пять тактик и техник матрицы MITRE ATT&CK, чаще всего обнаруживаемых профилями IDPS.
  - NGFW. IDPS. Top-5 Threats Type (Топ 5 типов угроз) – пять типов угроз, чаще всего обнаруживаемых профилями IDPS.
  - NGFW. IDPS. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями IDPS.

- NGFW. IDPS. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями IDPS.

- NGFW. File Web Antivirus. Top-5 Threats Name (Топ 5 названий угроз) – пять угроз, чаще всего обнаруживаемых профилями Антивируса.

- NGFW. File Web Antivirus. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями Антивируса.

- NGFW. File Web Antivirus. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями Антивируса.

- Макет **NGFW DNS Security**:

  - NGFW. DNS Security. Top-5 Threats for Blocked Addresses (Топ 5 угроз на заблокированных адресах) – пять наиболее частых угроз с IP-адресов, заблокированных профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Threats for Redirected Addresses (Топ 5 угроз на перенаправленных адресах) – пять наиболее частых угроз с IP-адресов, перенаправленных профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Redirected Hostnames (Топ 5 перенаправленных доменов) – пять доменов, наиболее часто перенаправляемых профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Source IP Addresses With the Most Redirected Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом перенаправленного веб-трафика) – пять IP-адресов источника, наиболее часто перенаправляемых профилями Защиты DNS-трафика.

- Макет **NGFW Web Control & URL Web Antivirus**:

  - NGFW. URL Web Antivirus. Top-5 Web Categories for Blocked URLs (Топ 5 веб-категорий заблокированных URL) – пять наиболее частых веб-категорий URL, заблокированных профилями Веб-антивируса.

  - NGFW. URL Web Antivirus. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов с наибольшим объемом трафика, заблокированного профилями Веб-антивируса.

  - NGFW. Web Control. Top-5 Categories of Sites With the Most Warning Web Traffic (Топ 5 категорий веб-сайтов с предупреждением для веб-трафика) – пять категорий веб-сайтов, для которых наиболее часто было показано предупреждение от профилей Веб-Контроля.

  - NGFW. Web Control. Top-5 Categories of Sites With the Most Blocked Web Traffic (Топ 5 категорий веб-сайтов с заблокированным веб-трафиком) – пять категорий веб-сайтов с наибольшим объемом веб-трафика, заблокированного профилями Веб-Контроля.

- NGFW. Web Control. Top-5 Destination IP Addresses With the Most Warning Web Traffic (Топ 5 IP-адресов назначения с предупреждением для веб-трафика) – пять IP-адресов назначения, для которых наиболее часто было показано предупреждение от профилей Веб-Контроля.

- NGFW. Web Control. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с заблокированным веб-трафиком) – пять IP-адресов назначения с наибольшим объемом веб-трафика, заблокированного Веб-Контроля.

- NGFW. Web Control. Top-5 Web Control Category Sources for Blocked Addresses (Топ 5 источников веб-категорий заблокированных адресов) – пять наиболее частых источников, от которых были получены веб-категории заблокированных URL.

- NGFW. Web Control. Top-5 Web Control Category Sources for Redirected Addresses (Топ 5 источников веб-категорий перенаправленных адресов) – пять наиболее частых источников, от которых были получены веб-категории перенаправленных URL.

- Макет **NGFW Firewall**:

  - NGFW. Top-5 Application Services by Sessions (Топ 5 прикладных сервисов по сессиям) – пять наиболее используемых прикладных сервисов по количеству сессий.

  - NGFW. Top-5 Application Services by Traffic, MB (Топ 5 прикладных сервисов по трафику, в МБ) – пять наиболее используемых прикладных сервисов по объему трафика, в МБ.

  - NGFW. Top-5 Application Protocols by Sessions (Топ 5 прикладных протоколов по количеству сессий) – пять наиболее используемых протоколов приложений по количеству сессий.

  - NGFW. Top-5 Application Protocols by Traffic, MB (Топ 5 прикладных протоколов по трафику, в МБ) – пять наиболее используемых протоколов приложений по объему трафика, в МБ.

  - NGFW. Top-5 Client Applications by Sessions (Топ 5 клиентских приложений по сессиям) – пять наиболее используемых клиентских приложений по количеству сессий.

  - NGFW. Top-5 Client Applications by Traffic, MB (Топ 5 клиентских приложений по трафику, в МБ) – пять наиболее используемых клиентских приложений по объему трафика, в МБ.

  - NGFW. Top-5 Source IP by Traffic, MB (Топ 5 IP-адресов источника по трафику, в МБ) – пять IP-адресов источника с наибольшим объемом трафика, в МБ.

  - NGFW. Top-5 Destination IP by Traffic, MB (Топ 5 IP-адресов назначения по трафику, в МБ) – пять IP-адресов назначения с наибольшим объемом трафика, в МБ.

  - NGFW. Top-5 Web Sites by Sessions (Топ 5 веб-сайтов по сессиям) – пять доменов с наибольшим количеством сессий.

  - NGFW. Top-5 Web Sites by Traffic, MB (Топ 5 доменов по трафику, в МБ) – пять доменов с наибольшим объемом трафика, в МБ.

По умолчанию для преднастроенных макетов указан период обновления **Никогда**. Вы можете изменять эти макеты при необходимости.

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Open Single Management Platform (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором виджетов. Таким образом, пользователь может просматривать указанную в виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с виджетами, например, добавлять или скрывать их. Поэтому нужно разместить в панели мониторинга все необходимые пользователю виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**.

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** в области **Общие функции: Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли** → **Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга невозможно.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с виджетами.

3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.

   На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.

4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также невозможно изменить панель мониторинга. После выключения параметра можно управлять виджетами.

5. Настройте внешний вид панели мониторинга. Набор виджетов, подготовленный на вкладке **Панель мониторинга**, доступен пользователю с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер виджетов, добавлять или удалять виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. Для этого на вкладке **Панель мониторинга** можно выполнять те же действия с виджетами, что и в разделе **Мониторинг** → **Панель мониторинга**:

   - Добавлять виджеты в панель мониторинга.
   - Скрывать виджеты, которые не нужны пользователю.
   - Перемещать виджеты в определенном порядке.
   - Изменять размер или внешний вид виджетов.
   - Изменять параметры виджетов.

6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Open Single Management Platform, в том числе изменять параметры безопасности и виджеты.

7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.

8. Если пользователь хочет просмотреть статистику поддерживаемых приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права для этого пользователя. После этого данные приложений "Лаборатории Касперского" отображаются у пользователя в виджетах этих приложений.

Теперь пользователь может входить в Open Single Management Platform под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты администрирования и защиты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в OSMP Console в разделе **Мониторинг** → **Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky EDR Expert имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов, редактировать шаблоны отчетов и удалять их.

Можно создавать отчеты на основе существующих шаблонов, экспортировать отчеты в файл и создавать задачи рассылки отчетов.

Шаблон отчета

Шаблоны отчетов используются для указания условий и данных, на основе которых будет сформирован отчет, а также для настройки периода формирования отчетов. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня могут создавать, изменять и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. В таблице содержится следующая информация:

- **Имя** – название шаблона отчета.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, расположенное над таблицей.

  > При поиске шаблонов отчетов используются регулярные выражения.

- **Тенант** – название тенанта, которому принадлежит шаблон отчета.
- **Последнее обновление** – дата и время последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

- **Создал** – имя пользователя, создавшего шаблон отчета.
- **Описание** – информация о шаблоне отчета, которую вы можете добавить при необходимости.
- **Теги** – теги для поиска шаблона отчета. Вы можете искать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.
- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.
- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.
- **Название пакета** – название пакета инструментов, предназначенного для обработки событий.
- **Отправить по электронной почте** – метка о настроенном уведомлении пользователей по почте о сформированных отчетах.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора шаблона отчета в списке вы можете нажать на значок меню ⋮, чтобы открыть раскрывающийся список с доступными действиями:

- **Показать зависимости** – используйте это действие, чтобы открыть окно графа зависимостей для выбранного шаблона отчета. При необходимости в окне графа можно скачать данные о зависимостях в формате SVG и настроить фильтры для показа зависимостей на графе.
- **Показать историю версий** – используйте это действие, чтобы посмотреть историю версий интересующего вас шаблона отчета. При необходимости в открывшейся боковой панели вы можете сравнить версии между собой и восстановить ранее использованную версию.
- **Запустить отчет** – используйте это действие, чтобы сформировать отчет. Созданные отчеты отображаются на вкладке **Сформированные отчеты**.
- **Показать все сформированные отчеты** – используйте это действие, чтобы посмотреть список всех отчетов, сформированных по выбранному шаблону отчета. При необходимости вы можете сохранить выбранный отчет в одном из поддерживаемых форматов или удалить отчет.
- **Изменить расписание** – используйте это действие, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.

Вы также можете посмотреть доступный вам список шаблонов отчетов в разделе **Ресурсы** → **Список**. Для этого требуется выбрать **Шаблон отчетов** в столбце **Тип ресурса**.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Введите название отчета и выберите тип отчета.

4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.

5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:

   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.

6. Нажмите на кнопку **OK**, чтобы завершить работу мастера.

7. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

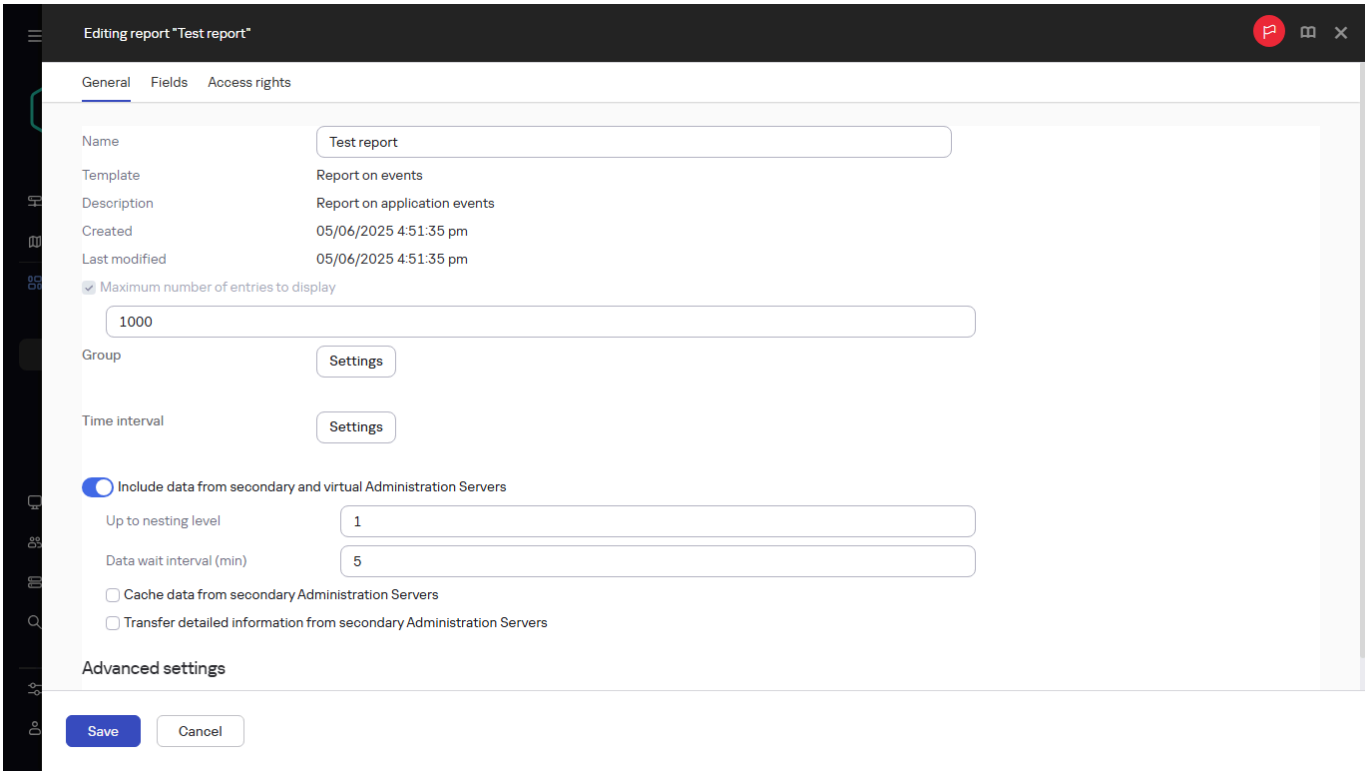
1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.

2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.

   В качестве альтернативы можно сначала сформировать отчет, а затем нажать на кнопку **Изменить**.

3. Нажмите на кнопку **Открыть свойства шаблона отчета**.

Откроется окно **Изменение отчета <имя отчета>** на вкладке **Общие**.



Свойства шаблона отчета

4. Измените свойства шаблона отчета:

- Вкладка **Общие**:

  - Название шаблона отчета

  - **Максимальное число отображаемых записей**

    Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение. Обратите внимание, что этот параметр не влияет на максимальное количество событий, которые вы можете включить в отчет при экспорте отчета в файл.

    Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Поля** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

    Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

    По умолчанию параметр включен. По умолчанию указано значение 1000.

  - **Группа**

    Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

- **Период**

  Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

  - между двумя указанными датами;
  - от указанной даты до даты создания отчета;
  - от даты создания отчета минус указанное количество дней до даты создания отчета.

- **Включать данные подчиненных и виртуальных Серверов администрирования**

  Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

  Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

  По умолчанию параметр включен.

- **До уровня вложенности**

  Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

  По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Вкладка **Поля**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

  В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

  Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Удаление шаблонов отчетов

Чтобы удалить шаблоны отчетов:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.

2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

Универсальность шаблона отчетов

Шаблон отчета в KUMA считается универсальным, если создается в тенанте Shared. Шаблоны отчетов, созданные в других тенантах, являются неуниверсальными.

Для работы с универсальным шаблоном отчета у пользователя должны быть следующие роли:

- Для создания, изменения параметров и удаления нужна роль Редактирование общих ресурсов. При наличии такой роли пользователь получает доступ ко всем общим ресурсам.

  Если роль пользователя предполагает работу с ресурсами КИИ, то признак КИИ может установить любой пользователь с ролью Редактирование общих ресурсов.

- Для просмотра списка универсальных шаблонов отчетов нужна роль Чтение общих ресурсов. При наличии таких прав пользователь получает доступ на чтение всех общих ресурсов.

Виджеты в универсальном шаблоне отчета отображаются с учетом следующего:

- Данные виджетов для тенантов отображаются в соответствии с доступом пользователя к тенантам, глобальным фильтром тенантов и конфигурацией шаблона отчетов или виджета.

- Данные виджетов при изменении параметров шаблона отчета можно посмотреть с помощью кнопки **Обновить предпросмотр**.

- Данные виджетов по событиям поступают из базы данных в соответствии с параметрами набора пространств пользователя. Если при формировании отчета оказывается, что у пользователя нет доступа к пространствам одного или нескольких тенантов, KUMA сформирует пустой отчет и отобразится сообщение о невозможности предоставления других результатов из-за отсутствия доступа к нужным пространствам.

- Данные виджетов в отчете могут формироваться с учетом КИИ или без учета КИИ. Для доступа к отчетам, в которых данные рассчитывались с учетом КИИ, у пользователя должна быть роль Доступ к КИИ.

- К универсальным отчетам применимы ограничения для виджетов активных листов и контекстных таблиц.

Экспорт отчета в файл

Вы можете сохранить один или несколько отчетов в форматах XML, HTML или PDF. Open Single Management Platform позволяет экспортировать до 10 отчетов в файлы указанного формата одновременно.

> Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

Чтобы экспортировать отчет в файл:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.

2. Выберите отчеты, которые вы хотите экспортировать.

   Если вы выберете более десяти отчетов, кнопка **Экспортировать отчет** будет неактивна.

3. Нажмите на кнопку **Экспортировать отчет**.

4. В открывшемся окне настройте следующие параметры экспорта:

- **Имя файла**.

  Если вы выбрали один отчет для экспорта, укажите имя файла отчета.

  Если вы выбрали несколько отчетов, имена файлов отчетов будут совпадать с именами выбранных шаблонов отчетов.

- **Максимальное количество записей**.

  Укажите максимальное количество записей, которые будут включены в файл отчета. По умолчанию указано значение 10 000.

  Вы можете экспортировать отчет с неограниченным количеством записей. Обратите внимание, что если ваш отчет содержит большое количество записей, время, необходимое для создания и экспорта отчета, увеличивается.

- **Формат файла**.

  Выберите формат файла отчета: XML, HTML, или PDF. При экспорте нескольких отчетов все выбранные отчеты сохраняются в указанном формате в виде отдельных файлов.

  Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

  Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF подчиненный Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

5. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет сохранен в файл в указанном формате.

Генерация и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.

2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

В отчете отображаются следующие данные:

- На вкладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета.
- На вкладке **Подробнее** отобразится таблица с подробными данными отчета.

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

Чтобы создать задачу рассылки отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.
2. Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Создать задачу рассылки отчетов**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку Далее.
4. На шаге мастера **Параметры новой задачи** введите название задачи.

   Название задачи по умолчанию – **Рассылка отчетов.** Если задача с таким названием уже существует, к названию задачи добавляется порядковый номер (<N>).
5. На шаге мастера **Конфигурация отчета** укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей.
   b. Формат отчета: HTML, XLS или PDF.

      Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.
   c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.

      Вы можете указать до 20 адресов электронной почты. Чтобы разделить адреса электронной почты, нажмите на клавишу **Enter**. Вы также можете вставить список адресов электронной почты, разделенных запятыми, и нажать на клавишу **Enter**.
   d. Будут ли отчеты сохраняться в папку вместе с соответствующими параметрами.

      После того как вы включите параметр **Сохранить в папке**, вам нужно указать POSIX-путь к папке. Если вы хотите сохранить отчеты в папку общего доступа, вам также нужно установить флажок **Задать учетную запись для доступа к папке общего доступа** и указать учетную запись пользователя и пароль для доступа к этой папке.

Если вы выбрали сохранение отчетов в папку общего доступа, требуется обеспечить доступ к этой папке с устройства, на котором установлен Сервер администрирования. Способы обеспечения доступа к папке и используемые инструменты зависят от вашей инфраструктуры.

При сохранении отчетов в локальную папку обычно не требуются учетные данные, поскольку учетная запись, под которой работает Сервер администрирования, имеет доступ к этой папке. При необходимости вы можете указать учетные данные пользователя на шаге мастера **Выбор учетной записи для запуска задачи**.

Если вы хотите, чтобы новый файл отчета перезаписывал файл, который был сохранен в папке отчетов при предыдущем запуске задачи, вы можете установить флажок **Замещать предыдущие отчеты того же типа**, независимо от выбранной папки.

6. На шаге мастера **Настройка расписания запуска задачи** выберите расписание запуска задачи.

Доступны следующие варианты расписания запуска задачи:

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

  По умолчанию задача запускается каждую пятницу в текущее системное время.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **В указанные дни**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

  При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

  - Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
  - Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

    По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
  - Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

7. На этом шаге мастера настройте другие параметры расписания запуска задачи:

- В разделе **Расписание задачи** проверьте или перенастройте ранее выбранное расписание и установите период, дни месяца или недели, задайте условие вирусной атаки или выполнение другой задачи в качестве запуска задачи. В этом разделе также можно указать время запуска, если выбрано подходящее расписание.

- В разделе **Дополнительные параметры** укажите следующие параметры:

  - **Запускать пропущенные задачи**

    Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

    Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

    Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

    По умолчанию параметр включен.

  - **Использовать автоматическое определение случайного интервала между запусками задачи**

    Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

    Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

    По умолчанию параметр включен.

  - **Использовать автоматическую случайную задержку запуска задачи в интервале**

    Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

    По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

  - **Остановить, если задача выполняется дольше**

    По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

    Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

    По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

8. На шаге мастера **Выбор учетной записи для запуска задачи** укажите учетные данные учетной записи, которая используется для запуска задачи.

9. Если требуется изменить другие параметры задачи после ее создания, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**. По умолчанию параметр включен.

10. Нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

    Будет создана задача отправки отчета. Если параметр **Открыть окно свойств задачи после ее создания** включен, откроется окно параметров задачи.

Отчеты обнаружения и реагирования

Вы можете настроить регулярное формирование отчетов о состоянии процессов и объектов в KUMA.

Отчеты формируются с помощью *шаблонов отчетов*. Шаблоны отчетов находятся в разделе **Отчеты** на вкладке **Шаблоны**.

Сформированные отчеты хранятся в разделе **Отчеты** на вкладке **Сформированные отчеты**.

Чтобы сохранять сформированные отчеты в форматах HTML и PDF необходимо установить требуемые пакеты на устройстве с Ядром KUMA.

При развертывании KUMA в отказоустойчивом варианте временная зона сервера Ядра KUMA и время в браузере пользователя могут различаться. Это различие проявляется в расхождении времени, которое проставляется в отчетах, сформированных по расписанию, и данных, которые пользователь может экспортировать из виджетов. Чтобы избежать расхождения, рекомендуется настроить расписание формирования отчетов с учетом разницы временной зоны пользователей и временем UTC.

https://www.youtube.com/watch?v=3uapwg0Pq04

Шаблон отчета

Шаблоны отчетов используются для указания условий и данных, на основе которых будет сформирован отчет, а также для настройки периода формирования отчетов. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня могут создавать, изменять и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. В таблице содержится следующая информация:

- **Имя** – название шаблона отчета.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, расположенное над таблицей.

  > При поиске шаблонов отчетов используются регулярные выражения.

- **Тенант** – название тенанта, которому принадлежит шаблон отчета.

- **Последнее обновление** – дата и время последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

- **Создал** – имя пользователя, создавшего шаблон отчета.

- **Описание** – информация о шаблоне отчета, которую вы можете добавить при необходимости.

- **Теги** – теги для поиска шаблона отчета. Вы можете искать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.

- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.

- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.

- **Название пакета** – название пакета инструментов, предназначенного для обработки событий.

- **Отправить по электронной почте** – метка о настроенном уведомлении пользователей по почте о сформированных отчетах.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора шаблона отчета в списке вы можете нажать на значок меню ⋮, чтобы открыть раскрывающийся список с доступными действиями:

- **Показать зависимости** – используйте это действие, чтобы открыть окно графа зависимостей для выбранного шаблона отчета. При необходимости в окне графа можно скачать данные о зависимостях в формате SVG и настроить фильтры для показа зависимостей на графе.

- **Показать историю версий** – используйте это действие, чтобы посмотреть историю версий интересующего вас шаблона отчета. При необходимости в открывшейся боковой панели вы можете сравнить версии между собой и восстановить ранее использованную версию.

- **Запустить отчет** – используйте это действие, чтобы сформировать отчет. Созданные отчеты отображаются на вкладке **Сформированные отчеты**.

- **Показать все сформированные отчеты** – используйте это действие, чтобы посмотреть список всех отчетов, сформированных по выбранному шаблону отчета. При необходимости вы можете сохранить выбранный отчет в одном из поддерживаемых форматов или удалить отчет.

- **Изменить расписание** – используйте это действие, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.

Вы также можете посмотреть доступный вам список шаблонов отчетов в разделе **Ресурсы** → **Список**. Для этого требуется выбрать **Шаблон отчетов** в столбце **Тип ресурса**.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. Откройте Консоль OSMP и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.

   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В зависимости от выбранного раздела выполните одно из следующих действий:

   - В разделе **Отчеты** → **Шаблоны** нажмите на кнопку **Создать**, расположенную над таблицей со списком шаблонов отчетов.

   - В разделе **Ресурсы** → **Список** нажмите на кнопку **Создать** и выберите **Шаблон отчетов** в списке ресурсов.

3. В открывшемся окне укажите уникальное название шаблона отчета. Название должно содержать от 1 до 128 символов Юникода.

   Пользовательские шаблоны отчетов не могут иметь названия предустановленных шаблонов отчетов в тенанте Main.

   При попытке создать шаблон отчетов с названием предустановленного шаблона отчетов или присвоить пользовательскому шаблону отчетов имя предустановленного шаблона отчетов в тенанте Main вернется ошибка. В других тенантах, помимо тенанта Main, можно создать или дублировать пользовательский шаблон отчетов с именем предустановленного шаблона отчетов. Рекомендуется использовать пользовательские имена для пользовательских шаблонов отчетов.

4. В раскрывающемся списке **Тенант шаблона** выберите тенант, которому будет принадлежать создаваемый шаблон отчета.

5. В раскрывающемся списке **Собирать данные от тенантов** выберите один или несколько тенантов. На основании данных выбранных тенантов далее будут сформированы отчеты.

6. При необходимости в раскрывающемся списке **Период** выберите период, по которому требуется аналитика, одним из следующих способов:

   - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

     Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

   - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

     В формулах относительного периода используйте параметр now для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

     > Поле **От** является обязательным, и его значение не может превышать значение, установленное в поле **До**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **До**, параметр **now** указывается автоматически.

По умолчанию выбран относительный период **1 день (now-1d)**. Границы периода включаются. Например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 сегодняшнего дня.

Время в KUMA хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

7. При необходимости в поле **Срок хранения** укажите, в течение какого времени следует хранить сформированные по этому шаблону отчеты.

   Значение по умолчанию – 3 месяца.

8. При необходимости в раскрывающемся списке **Теги** выберите нужные теги для шаблона отчета.

9. При необходимости добавьте описание шаблона отчета.

10. С помощью переключателя **КИИ статус** включите отображение данных об активах, алертах и инцидентах, имеющих отношение к критической информационной инфраструктуре (КИИ). При этом отчеты, в которых данные рассчитывались с учетом КИИ, будут доступны для просмотра только пользователям, в параметрах которых установлен флажок **Доступ к объектам КИИ**.

    Если переключатель выключен, в виджетах отчетов не будут отображаться данные об активах, алертах и инцидентах, относящихся к КИИ, даже если у пользователя есть доступ к объектам КИИ.

11. Нажмите на кнопку **Сохранить**.

12. В открывшемся окне при необходимости можно поменять логотип шаблона отчетов, нажав на ссылку **Загрузите файл**. В окне загрузки укажите файл изображения для логотипа. Изображение должно быть в формате JPG, PNG или GIF и размером не более 3 МБ.

    Добавленный логотип будет отображаться в отчете вместо логотипа KUMA.

13. Нажмите на кнопку **Добавить виджет** и выберите требуемый виджет. В открывшемся окне настройте параметры выбранного виджета.

14. Вы можете добавить несколько виджетов. Виджеты можно перетаскивать по окну с помощью значка перетаскивания (⠿), расположенного рядом с левым верхним углом виджета. Если вам необходимо изменить размер виджета, вы можете сделать это с помощью значка растяжения (⤡), который появляется при наведении указателя мыши на правый нижний угол виджета.

15. Для виджетов с типами графиков **Круговая диаграмма**, **Столбчатая диаграмма**, **Линейная диаграмма**, **Счетчик** и **Календарная диаграмма** существуют следующие ограничения:

    - В запросах `SELECT` можно использовать поля расширенной схемы событий с типами `Строка`, `Число` и `Число с плавающей точкой`.

    - В запросах `WHERE` можно использовать поля расширенной схемы событий со всеми типами (`Строка`, `Число`, `Число с плавающей точкой`, `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой`).

    Для виджетов с типом графика `Таблица` в запросах `SELECT` можно использовать поля расширенной схемы событий со всеми типами (`Строка`, `Число`, `Число с плавающей точкой`, `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой`).

16. Нажав на значок меню ⋮ в правом верхнем углу виджета, вы можете выполнять следующие действия с виджетами:

    - изменять параметры виджетов;
    - создавать копии виджетов;
    - удалять виджеты;
    - загружать данные виджетов в формате .csv.

17. Нажмите на кнопку **Создать**.

    Новый шаблон отчета создан и отображается в Консоли OSMP на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список**. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, нужно настроить расписание.

Настройка расписания отчетов

Чтобы настроить расписание отчетов:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице со списком шаблонов отчета выберите шаблон отчета и нажмите на значок меню ⋮.
3. В раскрывающемся списке выберите **Изменить расписание**.

   Откроется окно **Изменить расписание**.

4. Если вы хотите, чтобы отчет формировался регулярно:

   a. Включите переключатель **Отправить отчет по расписанию**.

   b. В группе параметров **Повторять каждый** укажите периодичность формирования отчетов.

      Периодичность формирования отчетов можно указать по дням, неделям, месяцам или годам. В зависимости от выбранного периода требуется задать время, день недели, число месяца или дату формирования отчета.

   c. В поле **Время** укажите время, когда должен быть сформирован отчет.

   d. В раскрывающемся списке **Часовой пояс** выберите часовой пояс для определения времени отправки отчета.

5. В блоке **Настройки уведомлений** укажите следующие параметры:

   a. В раскрывающемся списке **Шаблон уведомления** выберите форму уведомления, которое будет направляться пользователю по расписанию.

   b. В группе настроек **Отправить** нажмите **Добавить**.

c. В открывшемся окне добавьте группу пользователей для отправки отчета и выберите нужный вам формат. Для этого выполните следующие действия:

- В раскрывающемся списке **Адреса электронной почты** выберите адреса электронной почты получателей отчета.
- В раскрывающемся списке **Формат** выберите формат отчета. Для выбора доступны следующие форматы: PDF, HTML, CSV, разделенный CSV, Excel.

Вы можете добавить несколько групп пользователей для отправки отчета, нажав на кнопку **Добавить группу**.

Отчеты будут отправлены по указанным адресам каждый раз, когда вы сформируете отчет вручную или KUMA сформирует отчет автоматически по расписанию.

> Чтобы сформированные отчеты можно было отправлять по электронной почте, нужно настроить SMTP-соединение.

Если получатели, которым отчет пришел на электронную почту, являются пользователями KUMA, они смогут скачать отчет или просмотреть отчет по ссылкам из письма. Если адресаты не являются пользователями KUMA, переход по ссылкам будет доступен, но авторизоваться в KUMA адресаты не смогут, поэтому им будут доступны только вложения.

Рекомендуется просматривать отчеты в формате HTML по ссылкам в веб-интерфейсе, поскольку при некоторых значениях разрешения экрана HTML-отчет из вложения может отображаться некорректно.

Вы можете отправить письмо без вложений, тогда получателям будут доступны отчеты только по ссылкам и только с аутентификацией в KUMA, без ограничений по ролям или тенантам.

d. Нажмите на кнопку **Добавить**.

6. Нажмите на кнопку **Сохранить**.

Расписание отчетов настроено.

Изменение шаблона отчета

Чтобы изменить шаблон отчета:

1. Откройте веб-интерфейс KUMA и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.
   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В зависимости от выбранного раздела выполните одно из следующих действий:

   - В разделе **Отчеты** → **Шаблоны** нажмите имя шаблона отчетов в таблице со списком шаблонов отчетов.
   - В разделе **Ресурсы** → **Список** нажмите на значок изменения параметров ( ) рядом с именем шаблона отчетов в списке ресурсов.

Откроется окно **Изменить шаблон**.

Это окно также можно открыть на вкладке Отчеты → Сформированные отчеты, выбрав существующий отчет и нажав на кнопку Изменить шаблон.

> Это окно также можно открыть на вкладке **Отчеты** → **Сформированные отчеты**, выбрав существующий отчет и нажав на кнопку **Изменить шаблон**.

3. Внесите необходимые изменения:

   - Измените название шаблона отчета.
   - Измените список тенантов, которые передают данные для отчета.
   - Нажмите на кнопку **Параметры** для изменения периода получения аналитических данных, срока хранения, тегов и описания шаблона отчета.
   - Нажмите на кнопку **Добавить виджет** для добавления виджета в шаблон отчета.
   - Нажмите на значок меню (⋮) для просмотра списка отчетов, сформированных по этому шаблону, или для удаления шаблона отчета.
   - Измените логотип отчета, загрузив его по ссылке **Загрузите файл**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.
   - Измените расположение виджетов, перетаскивая их.
   - Измените размер виджетов с помощью значка растяжения (⤡), который появляется при наведении указателя мыши на виджет.
   - С помощью значка меню (⋮) на виджете измените параметры виджетов, создайте копии виджетов, удалите виджеты или загрузите данные виджетов в формате CSV.

4. Нажмите на кнопку **Сохранить**.

   Шаблон отчета изменен и отображается в веб-интерфейсе KUMA на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список**.

Копирование шаблона отчета

Чтобы создать копию шаблона отчета:

1. Откройте веб-интерфейс KUMA и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.
   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В таблице выберите шаблон отчета и нажмите на кнопку **Дублировать**, расположенную над таблицей.

3. В открывшемся окне укажите название шаблона отчета. При копировании шаблона отчета в названии отчета появляется упоминание о копировании.

4. В раскрывающемся списке **Тенант шаблона** выберите тенанты, которым будет принадлежать копируемый шаблон отчета.

5. В раскрывающемся списке **Собирать данные от тенантов** выберите один или несколько тенантов, данные из которых будут представлены в шаблоне отчета.

6. При необходимости измените следующие параметры:

   - Период формирования отчета.
   - Срок хранения отчета.
   - Теги шаблона отчета.
   - Описание шаблона отчета.
   - Формирование данных в отчете с учетом КИИ.

7. Нажмите на кнопку **Сохранить**.

Копия шаблона отчета создана и отображается в веб-интерфейсе KUMA на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список**.

Удаление шаблона отчета

Чтобы удалить шаблон отчета:

1. Откройте веб-интерфейс KUMA и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.
   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В таблице шаблонов отчетов с помощью флажка выберите шаблон отчета и нажмите на кнопку **Удалить**, расположенную над таблицей.

   Откроется окно подтверждения.

3. Выполните одно из следующих действий:

   - Если вы хотите удалить только шаблон отчета, нажмите на кнопку **Удалить**.
   - Если вы хотите удалить шаблон отчета и все отчеты, сформированные с помощью этого шаблона, нажмите **Удалить с отчетами**.

Шаблон отчета удален.

Экспорт и импорт шаблона отчета

Чтобы экспортировать шаблон отчета:

1. Откройте веб-интерфейс KUMA и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.
   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в KUMA.

2. С помощью флажка выберите шаблон отчета для экспорта.
3. Нажмите на кнопку **Экспортировать**, расположенную над таблицей со списком шаблонов отчетов.
4. В открывшейся боковой панели выполните следующие действия:

   a. Укажите пароль к файлу с экспортируемыми ресурсами. Пароль должен удовлетворять следующим требованиям:

      - длина минимум 16 символов;
      - хотя бы один символ в нижнем регистре;
      - хотя бы один символ в верхнем регистре;
      - хотя бы одна цифра;
      - хотя бы один специальный символ.

   b. В раскрывающемся списке **Тенант** выберите тенант, из которого вы хотите экспортировать выбранные ресурсы.

   c. С помощью флажков укажите ресурсы, которые вы хотите экспортировать.

      Если вы установите флажок **Все ресурсы**, экспортироваться будут все ресурсы, находящиеся в папках выбранного тенанта.

5. Нажмите на кнопку **Экспортировать**.

При экспорте шаблонов отчета необходимо учитывать следующее:

- Шаблоны отчетов экспортируются без информации о тенантах, хранилищах и пространствах, поскольку эти параметры настраиваются индивидуально для каждого экземпляра KUMA.
- Виджеты шаблона отчета также экспортируются без информации о тенантах, хранилищах и пространствах.

Чтобы импортировать шаблон отчета:

1. Откройте веб-интерфейс KUMA и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.

   - **Ресурсы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в KUMA.

2. С помощью флажка выберите шаблон отчета для импорта.

3. Нажмите на кнопку **Импортировать**, расположенную над таблицей со списком ресурсов.

4. В открывшейся боковой панели в раскрывающемся списке **Тенант** выберите тенант, в который вы хотите импортировать шаблон отчета.

5. Выберите источник импорта: **Файл** или **Репозиторий**.

6. В зависимости от выбранного источника импорта, выполните следующие шаги:

   a. Если вы выбрали **Файл** в качестве источника импорта, выполните следующие действия:

      - Укажите пароль к импортируемому файлу.

      - С помощью кнопки **Выбрать файл** выберите файл для импорта.

      - С помощью флажков выберите ресурсы, которые вы хотите импортировать.

   b. Если вы выбрали **Репозиторий** в качестве источника импорта, в открывшейся таблице выберите один или несколько пакетов репозитория.

7. Нажмите на кнопку **Импортировать**.

8. При необходимости устраните конфликты между импортированными из файла и существующими ресурсами.

При импорте шаблона отчета необходимо учитывать следующее:

- Если шаблон импортируется в любой тенант, то тенант импортируемого шаблона отчета указывается в качестве тенанта ресурса и тенанта источника данных.

- После импорта ресурсов необходимо указать пространства для виджетов с событиями и при необходимости расширить список тенантов.

Универсальность шаблона отчетов

Шаблон отчета в KUMA считается универсальным, если создается в тенанте Shared. Шаблоны отчетов, созданные в других тенантах, являются неуниверсальными.

Для работы с универсальным шаблоном отчета у пользователя должны быть следующие роли:

- Для создания, изменения параметров и удаления нужна роль Редактирование общих ресурсов. При наличии такой роли пользователь получает доступ ко всем общим ресурсам.

  Если роль пользователя предполагает работу с ресурсами КИИ, то признак КИИ может установить любой пользователь с ролью Редактирование общих ресурсов.

- Для просмотра списка универсальных шаблонов отчетов нужна роль Чтение общих ресурсов. При наличии таких прав пользователь получает доступ на чтение всех общих ресурсов.

Виджеты в универсальном шаблоне отчета отображаются с учетом следующего:

- Данные виджетов для тенантов отображаются в соответствии с доступом пользователя к тенантам, глобальным фильтром тенантов и конфигурацией шаблона отчетов или виджета.

- Данные виджетов при изменении параметров шаблона отчета можно посмотреть с помощью кнопки **Обновить предпросмотр**.

- Данные виджетов по событиям поступают из базы данных в соответствии с параметрами набора пространств пользователя. Если при формировании отчета оказывается, что у пользователя нет доступа к пространствам одного или нескольких тенантов, KUMA сформирует пустой отчет и отобразится сообщение о невозможности предоставления других результатов из-за отсутствия доступа к нужным пространствам.

- Данные виджетов в отчете могут формироваться с учетом КИИ или без учета КИИ. Для доступа к отчетам, в которых данные рассчитывались с учетом КИИ, у пользователя должна быть роль Доступ к КИИ.

- К универсальным отчетам применимы ограничения для виджетов активных листов и контекстных таблиц.

Сформированные отчеты

Все отчеты формируются с помощью шаблонов отчетов. Сформированные отчеты доступны на вкладке **Сформированные отчеты** в разделе **Отчеты** и отображаются в таблице со следующей информацией:

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов по их названию, используя поле **Поиск**, расположенное над таблицей.

- **Период** – период времени, за который была извлечена аналитика отчета.

- **Последний отчет** – дата и время формирования последнего отчета.

- Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

- **Тенант** – название тенанта, которому принадлежит отчет.

- **Пользователь** – имя пользователя, который сформировал отчет вручную. Если отчет был сформирован по расписанию, значение будет пустым. Если отчет был сформирован в версии KUMA ниже 2.1, значение будет пустым.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора отчета в списке сформированных отчетов вы можете выполнить следующие действия с отчетами:

- Создать отчет.
- Открыть и просмотреть отчет.
- Сохранить сформированный отчет в нужном формате. Доступные форматы: HTML, PDF, CSV, разделенный CSV, Excel. По умолчанию во всех форматах выводится 250 строк. Максимальное количество строк, которые могут отображаться в таблицах в форматах PDF и HTML равно 500. Если вы хотите выводить в отчет более 500 строк, задайте в SQL-запросе желаемое значение параметра LIMIT и сохраните отчет в формате CSV.
- Настроить параметры шаблона отчета.
- Удалить отчет.

Просмотр отчетов

Чтобы просмотреть отчет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчетов нажмите на название сформированного отчета.

   Откроется новая вкладка браузера с виджетами, отображающими аналитику отчетов. Если виджет отображает данные о событиях, алертах, инцидентах или активных листах, при нажатии на его заголовок открывается соответствующий раздел веб-интерфейса KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета. К виджетам применяются значения по умолчанию.

   Если вы хотите просмотреть полные данные, выгрузите отчет в формате CSV с указанными параметрами из запроса.

   Если вы в настройке виджета включили переключатель **Итоговые значения**, на виджете отображается значение **Всего**, но при вложении или выгрузке отчета в форматах CSV и расширенный CSV значение **Всего** не отображается. Для отображения значения **Всего** в отчете, вы можете воспользоваться формулами Excel или переписать итоговое значение с виджета, или воспользоваться вложениями в формате PDF и HTML.
3. При необходимости сохраните отчет в выбранном формате с помощью кнопки **Сохранить как**.

Создание отчетов

Вы можете создать отчет вручную или настроить расписание, чтобы отчеты создавались автоматически.

Чтобы создать отчет вручную:

1. Откройте веб-интерфейс KUMA и перейдите в раздел **Отчеты**.
2. Выполните одно из следующих действий:
   a. На вкладке **Сформированные отчеты** выполните следующие действия:
      - С помощью флажка выберите отчет в таблице со списком отчетов.
      - Нажмите на кнопку **Сформировать отчет**, расположенную над таблицей.
   b. На вкладке **Шаблоны**:
      - С помощью флажка выберите отчет в таблице со списком шаблонов отчета.
      - Нажмите на значок меню ⋮ и выберите в раскрывающемся списке **Сформировать отчет**.

   В течение 15 секунд отчет будет создан и помещен на вкладку Отчеты → Сформированные отчеты.

Вы также можете настроить расписание отчетов для автоматического формирования отчетов.

Сохранение отчетов

Чтобы сохранить отчет в нужном формате:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. С помощью флажка выберите сформированный отчет в таблице со списком сформированных отчетов.
3. В раскрывающемся списке **Сохранить как**, расположенном над таблицей, выберите нужный формат: HTML, PDF, CSV, разделенный CSV, Excel.

   Отчет сохраняется в папку загрузки, настроенную в вашем браузере.

Отчет также можно сохранить в выбранном формате при просмотре.

Обновление отчетов

Чтобы обновить сформированный отчет:

1. Откройте веб-интерфейс KUMA и перейдите в раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице со списком сформированных отчетов выберите интересующий вас отчет.
3. Нажмите на кнопку **Сформировать отчет**, расположенную над таблицей.

   Отчет обновится в течение 15 секунд и будет доступен в разделе **Отчеты** → **Сформированные отчеты**.

Удаление отчетов

Чтобы удалить отчет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице со списком сформированных отчетов выберите интересующий вас отчет.
3. Нажмите на кнопку **Удалить**, расположенную над таблицей.

   Откроется окно подтверждения.
4. Нажмите на кнопку **Удалить**.

   Выбранный отчет удален.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky EDR Expert, и об управлении блокировкой частых событий.

О событиях в Kaspersky EDR Expert

Kaspersky EDR Expert позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

События по типу

В Kaspersky EDR Expert существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky EDR Expert:
  - Сервер администрирования
  - Агент администрирования
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

События по уровню важности

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky EDR Expert. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

События компонентов Kaspersky EDR Expert

Каждый компонент Kaspersky EDR Expert имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования и Агенте администрирования. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Kaspersky EDR Expert, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky EDR Expert и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий: Настройка срока хранения события.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истек	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	180 дней
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Критический*.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Open Single Management Platform проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней невозможно изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky EDR Expert работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky EDR Expert проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky EDR Expert определяет правила генерации событий при превышении лицензионного ограничения.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky EDR Expert начинает работать в режиме базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: • Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky EDR Expert (добавьте действительный код активации или файл ключа на Сервер администрирования). • Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней
Срок действия MDM-сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	180 дней
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или файл ключа, который вы используете, в список запрещенных. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Kaspersky EDR Expert и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней
Вирусная атака	• 26 (для компонента Защита от файловых угроз) • 27 (для компонента Защита от почтовых угроз) • 28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверить, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверить, были ли изменены имя пользователя и/или пароль к папкам. • Проверить подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD_SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky EDR Expert вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлена СУБД. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования.	180 дней

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истекает	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	90 дней
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Не удалось выполнить тестовое подключение к SIEM-серверу	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают при сбое автоматической проверки подключения к SIEM-серверу.	90 дней
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно**. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью OSMP Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью OSMP Console.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Предупреждение*.	90 дней
Не удалось скачать файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Вы пытаетесь загрузить файл в корпоративный контейнер, но корпоративный контейнер не был создан. • На устройстве недостаточно места. • Не удалось скачать информацию о файле с сервера. • Не удалось скачать содержимое файла с сервера. • Не удалось создать папку на устройстве. • На личном устройстве отсутствует доступ к файлам. • В корпоративном контейнере отсутствует доступ к файлу.	90 дней
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes").	90 дней
Обнаружено получение частных событий		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней
Жесткий диск почти заполнен	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky EDR Expert проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky EDR Expert определяет правила генерации событий при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений скоро будет достигнуто ограничение числа установок	4128	KLSRV_INVLICPROD_EXPIRED_SOON	События этого типа возникают, когда истекает срок действия одного из лицензионных ключей сторонних приложений, входящих в группу лицензионных приложений. В результате число разрешенных установок для одной из групп будет уменьшено. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console.	90 дней
Недостаточно места в базе данных Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATED	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств обновлен	6127	KLSRV_EV_SRV_CERT_RENEWED	События этого типа возникают, если сертификат Сервера администрирования был обновлен.	30 дней
Аудит: Команда была отправлена на устройство	4170	KLAUD_EV_COMMAND_SENT	События этого типа возникают, если пользователь отправил команду на мобильное устройство.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT		30 дней
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	События этого типа возникают при подключении пользователя к Серверу администрирования с помощью OSMP Console. Такие события включают информацию об IP-адресе устройства, на котором установлен Сервер OSMP Console.	30 дней
Аудит: Ключи шифрования импортированы/экспортированы	5100	KLAUD_EV_DPEKEYSEXPORT	Например, это событие происходит во время переноса данных.	30 дней
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	События этого типа возникают при изменении группы безопасности.	30 дней
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • управляемых устройствах; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.	30 дней
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.	30 дней
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	Например, это событие возникает, если задача завершилась ошибкой.	30 дней
Аудит: Тестовое подключение к SIEM-серверу выполнено успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	События этого типа возникают при успешном подключении к SIEM-серверу.	30 дней
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	События этого типа возникают, если права пользователя были изменены.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 дней
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Подробнее см. в статье Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.	30 дней
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает обновление базы данных.	30 дней
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	События этого типа возникают, если устройства были перемещены в группы администрирования в соответствии с правилами перемещения устройств. Для каждого перемещенного устройства публикуется отдельное событие.	30 дней
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	События этого типа возникают, когда устройства были автоматически удалены из группы из-за неактивности.	30 дней
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	События этого типа возникают при изменении токена Firebase Cloud Messaging на устройстве. Информацию о ротации токенов FCM см. в документации сервиса Firebase.	30 дней
Файл загружен на Сервер администрирования	4162	KLSRV_FILE_UPLOADED	События этого типа возникают, если администратор загрузил файл в список в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**.	30 дней
Файл удален с Сервера администрирования	4163	KLSRV_FILE_REMOVED	События этого типа возникают, если администратор удалил файл из списка в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**.	30 дней
Файл загружен на устройство	4164	KLSRV_FILE_DOWNLOADED	События этого типа возникают в следующих случаях: • Администратор загрузил файл на свое рабочее место из списка в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**. • Файл из списка **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы** загружен на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось загрузить файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Произошла ошибка при попытке администратора загрузить файл на свое рабочее место из списка в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**. • Произошла ошибка при загрузке файла из списка **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы** на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	30 дней
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED		30 дней
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 90%	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	30 дней
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	События этого типа возникают при обнаружении новых сетевых устройств.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 90% от общего количества лицензионных единиц, охватываемых лицензией. Даже при превышении лицензионных ограничений клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky EDR Expert определяет правила генерации событий при превышении лицензионного ограничения.	30 дней
Резервный сертификат Сервера администрирования для мобильных устройств создан	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	События этого типа возникают, если сертификат Сервера администрирования создан.	30 дней
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает копирование файлов в указанную папку.	30 дней

События **Резервный сертификат создан** и **Сертификат обновлен** автоматически публикуются Сервером администрирования и отображаются в Консоли администрирования только при выполнении соответствующих этим событиям операций для сертификатов Сервера администрирования для мобильных устройств и устройств с защитой на уровне UEFI.

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	События этого типа возникают при сбое тестового соединения для настроенного подключения прокси-сервера KSN.	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	События этого типа возникают при обнаружении инцидента на устройстве. Например, это событие возникает, когда на устройстве мало места на диске.	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	События этого типа возникают, если есть несовпадение между файлом sudoers и референсным файлом.	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Например, события этого типа возникают, когда отклоняется Лицензионное соглашение для установки обновлений приложений сторонних производителей.	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	Общее событие предупреждения.	30 дней
Возвращено предупреждение во время установки обновления модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем критичности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Получен сертификат для HTTPS-порта Веб-сервера	—	WEB_SERVER_CERTIFICATE_RENEWED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Корневой сертификат установлен	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 дней
Корневые сертификаты удалены	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 дней
Файл sudoers успешно восстановлен до референсного значения	7725	KLNAG_EV_SUDOER_RESTORED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Управление учетными записями: информационные сообщения	7721	KLNAG_EV_USR_MNG_INF	30 дней
Веб-Сервер запущен на устройстве	—	WEB_SERVER_STARTED	30 дней
Веб-Сервер остановлен на устройстве	—	WEB_SERVER_STOPPED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней
Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней

Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе OSMP Console.

Выборки событий доступны в Консоли OSMP в разделе **Мониторинг** → **Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky EDR Expert имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные сообщения.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- **События аудита**.

В Kaspersky EDR Expert отображаются события аудита, связанные с операциями службы в Консоли OSMP. Эти события обусловлены действиями экспертов "Лаборатории Касперского". Такие события, например, включают: вход на Сервер администрирования; изменение портов Сервера администрирования; резервное копирование данных Сервера администрирования; создание, изменение и удаление учетных записей пользователей.

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий. В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky EDR Expert отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

Вы можете выполнить следующее:

- Изменить параметры выборки событий.
- Сгенерировать выборки событий.
- Просмотреть сведения о выбранных выборках событий.
- Удалить выборки событий.
- Удалить события из базы данных Сервера администрирования.

Создание выборки событий

Чтобы создать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.
5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.
6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

Изменение выборки событий

Чтобы изменить выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.

4. Отредактируйте свойства выборки событий.

> Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

Для пользовательских выборок можно изменять все свойства.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:
   - Чтобы настроить сортировку для результатов выборки событий:
     a. Нажмите на кнопку **Изменить сортировку и запустить**.
     b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.
     c. Нажмите на имя выборки.
   - В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.

Экспорт выборки событий

Open Single Management Platform позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

> Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Open Single Management Platform (предопределенные выборки), не может быть сохранен в файл.

Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.

2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Open Single Management Platform позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий и ее параметры.

Чтобы импортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.

2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.

3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

> Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

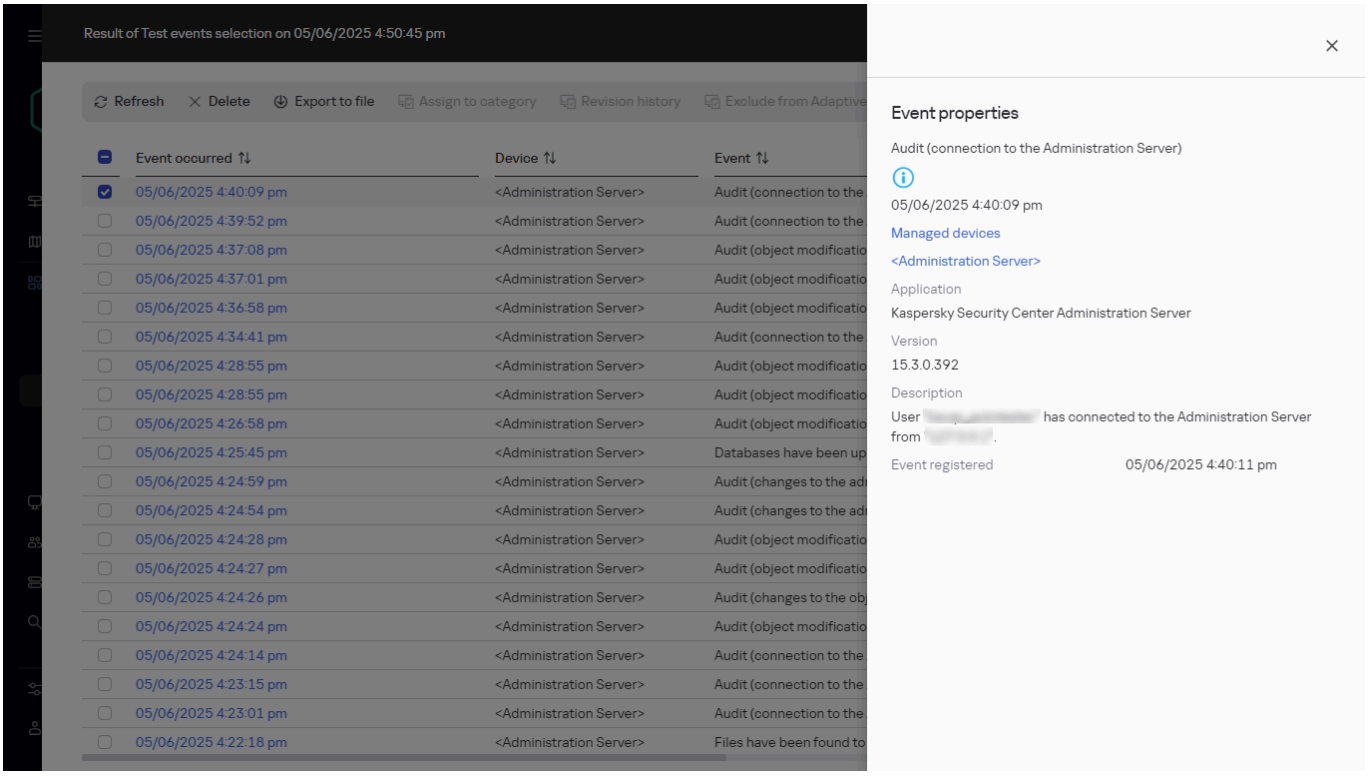
Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.

2. Нажмите на требуемое событие.

   Откроется окно **Свойства события**.



Окно свойств событий

3. В открывшемся окне можно выполнить следующие действия:

   - Просмотреть информацию выбранного события.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

Экспорт событий в файл

Open Single Management Platform позволяет сохранять события из выборки событий в файл TXT.

Чтобы экспортировать события в файл:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.

   Вы также можете выбрать несколько событий или всю выборку событий.
3. Нажмите на кнопку **Экспортировать в файл**.

Выбранные события будут экспортированы в файл формата TXT.

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями, вы можете перейти к истории ревизий объекта.

Чтобы просмотреть историю объекта из события:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

Удаление событий

Чтобы удалить события из выборки событий:

1. Запустите выборку событий.
2. Выберите события:
   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить**.

Чтобы удалить события из списка событий устройства:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Активы (Устройства)**.
   - Для нераспределенных устройств: **Управление активами** → **Нераспределенные устройства**.
2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.
3. Выберите события:
   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.
4. Нажмите **Удалить** и подтвердите действие.
5. В появившемся окне нажмите на кнопку **Удалить**.

   Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

   Выборка событий будет удалена.

Настройка срока хранения события

Kaspersky EDR Expert позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название требуемой политики.

   Вы можете выбрать политику управляемого приложения "Лаборатории Касперского", Агента администрирования или Сервера администрирования. Для Сервера администрирования вы можете настроить срок хранения событий, нажав на имя Сервера администрирования.
3. Выберите вкладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий. При необходимости вы можете перейти в раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
4. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите переключатель **Хранить в базе данных Сервера администрирования в течение (сут)**.
5. В поле редактирования под переключателем укажите количество дней для сохранения события.
6. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

   > Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования, вы не сможете изменить значение срока хранения события.
7. Нажмите на кнопку **OK**, а затем после того, как правая панель закроется, нажмите на кнопку **Сохранить**.

   Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Linux, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Чтобы узнать, заблокировано ли событие, вы можете просмотреть список уведомлений или просмотреть, присутствует ли это событие в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку частых событий.

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

Чтобы управлять блокировкой частых событий:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий**:

   - Если вы хотите разблокировать прием частых событий:

     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.

     b. Нажмите на кнопку **Сохранить**.

   - Если вы хотите заблокировать прием частых событий:

     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировать**.

     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.

4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Обработка и хранение событий на Сервере администрирования

Информация о событиях, возникших в работе приложения и управляемых устройств, сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Ретроскан

В обычном режиме коррелятор работает только с событиями, поступающими от коллекторов в реальном времени. **Ретроспективное сканирование** позволяет применить правила корреляции к произошедшим ранее событиям, если вы хотите отладить правила корреляции или проанализировать данные.

Чтобы проверить работу правила корреляции, не обязательно воспроизводить инцидент в реальном времени. Вы можете запускать правило корреляции в режиме **Ретроспективное сканирование** для существующих событий, среди которых есть нужный инцидент.

С помощью поискового запроса вы можете определить список событий, для которых будет выполнено ретроспективное сканирование, задать период поиска и указать хранилище, в котором нужно искать события. Можно настроить задачу таким образом, чтобы во время ретроспективного сканирования событий создавались алерты и применялись правила реагирования.

Чтобы включить ретроспективное сканирование:

1. В разделе **Мониторинг** → **Поиск угроз** веб-интерфейса решения получите необходимую выборку событий:
   - Выберите хранилище.

     Перед запуском ретроспективного сканирования убедитесь, что выбраны нужные кластеры и пространства.

- Настройте поисковое выражение с помощью конструктора или поискового запроса.

  Перед запуском ретроспективного сканирования убедитесь, что в поле SQL-запроса указано нужное выражение.

- Задайте необходимый период.

  Перед запуском ретроспективного сканирования убедитесь, что в поле периода выбран нужный период.

2. В раскрывающемся списке ··· выберите **Ретроспективное сканирование**.

   Откроется окно ретроспективного сканирования.

3. В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.

   Перед запуском ретроспективного сканирования проверьте количество событий, найденных при выполнении SQL-запроса. Эта информация отображается в блоке **Показать временную шкалу** → **Всего:**. Если в SQL-запросе не указано значение параметра **LIMIT**, в коррелятор отправляются все события за период и длительность выполнения задачи возрастает. Если в периоде установлен относительный период (например, *now-1h*), при запуске ретроспективного сканирования могут появится новые события, которые также будут отправлены в коррелятор. Если коррелятор установлен не в основных тенантах (Main, RootTenant), в него могут отправляться события только того тенанта, где он установлен.

4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, с помощью которых нужно обработать выбранные события. Если на этом шаге не выбрано ни одного правила, сканирование будет выполнено с применением всех правил корреляции.

5. В поле **EPS лимит** укажите максимальное количество EPS, которое используется при выполнении ретроспективного сканирования. Указанное значение определяет максимальную нагрузку при проведении ретроспективного сканирования. По умолчанию указано значение 0, то есть ограничения по EPS для ретроспективного сканирования отсутствуют.

   Для указания максимального количества EPS, которое используется при выполнении ретроспективного сканирования, не допускается использование отрицательных значений.

6. Если вы хотите, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.

7. Если вы хотите, чтобы в процессе обработки событий создавались алерты, включите переключатель **Создать алерты**.

8. Нажмите на кнопку **Создать задачу**.

Задача ретроспективного сканирования создана и отображается в разделе **Диспетчер задач**.

Чтобы просмотреть результаты сканирования, в разделе **Диспетчер задач** веб-интерфейса KUMA нажмите на созданную вами задачу и в раскрывающемся списке выберите **Перейти к событиям**.

> Результаты ретроспективного сканирования отображают только сформированные корреляционные события.
> Начало периода в результатах ретроспективного сканирования отображается как <дата и время создания задачи>, окончание периода – <дата и время создания задачи + один час> (или текущее время, если один час с момента создания задачи еще не истек).
> Если в результатах ретроспективного сканирования нет событий, значит в корреляторе не было срабатываний по отправленным в него событиям из SQL-выборки.

Откроется новая вкладка браузера с событиями, обработанными в ходе ретроспективного сканирования, а также агрегированными и корреляционными событиями, созданными во время обработки. Корреляционные события, созданные ретроспективным сканированием, имеют дополнительное поле ReplayID, в котором хранится уникальный идентификатор выполнения ретроспективного сканирования. Аналитик может повторно запустить ретроспективный поиск из контекстного меню задачи. У новых корреляционных событий будет другой ReplayID.

> В зависимости от параметров браузера может потребоваться подтверждение открытия вкладки с результатами ретроспективного сканирования. Подробнее см. в документации вашего браузера.

При ретроспективном сканировании события не обогащаются данными из CyberTrace и Kaspersky Threat Intelligence Portal.

Активные листы обновляются при ретроспективном сканировании.

> Ретроспективное сканирование невозможно проводить по SQL-запросам, содержащим арифметические выражения или только поля агрегации. Вы можете выполнить ретроспективное сканирование на группах событий, полученных с помощью SQL-запроса с группировкой данных, только после завершения выполнения запроса. Для этого сначала выполните SQL-запрос с группировкой данных и получите список групп событий, а затем запустите ретроспективное сканирование по одной из групп.

Уведомления и статусы устройств

В этом разделе содержится информация о том, как просматривать уведомления, настраивать доставку уведомлений, использовать статусы устройств и включать изменение статусов устройств.

Использование уведомлений

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

Экранные уведомления

Экранные уведомления предупреждают вас о событиях, сгруппированных по уровням важности (*Критическое уведомление*, *Предупреждающие уведомление*, и *Информационное уведомление*).

Экранные уведомления могут иметь один из двух статусов:

- *Просмотрено*. Это означает, что вы выполнили рекомендованное действие для уведомления или вы назначили этот статус для уведомления вручную.
- *Не просмотрено*. Это означает, что вы не выполнили рекомендуемое действие для уведомления или не назначили этот статус для уведомления вручную.

По умолчанию в список уведомлений входят уведомления со статусом *Не просмотрено*.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Kaspersky EDR Expert позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запустив исполняемый файл или скрипт.

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг** → **Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг** → **Панель мониторинга**. В этом виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.

2. На левой панели выберите одну из следующих категорий:

   - **Развертывание**.
   - **Устройства**.
   - **Защита**.
   - **Обновления**.

     Это уведомление включает в себя уведомления о доступных для скачивания приложениях "Лаборатории Касперского", уведомления об обновлении антивирусных баз, которые были загружены, а также уведомления об устройствах, если есть, которые требуют перезагрузки после обновления Агента администрирования.
   - **Защита от эксплойтов**.
   - **Сервер администрирования**.

     Это уведомление включает в себя события, относящиеся только к Серверу администрирования.

- **Полезные ссылки**.

  Это уведомление включает в себя ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию.

В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** (), **Предупреждающие уведомления** (), **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.
- **Уведомление**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить приложение безопасности на устройства, просмотреть список устройств или список событий. После того как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.
- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу Консоли OSMP.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите вкладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* () и *Предупреждающие уведомления* (). Список уведомление включает следующее:

   - Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
   - Значок, относящийся к теме уведомления: развертывание (), защита (), обновления(), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
   - Описание уведомления.
   - Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
   - Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
   - Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите вкладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на вкладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

Чтобы просмотреть экранные уведомления на виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить виджет**.

2. В открывшемся окне нажмите на категорию **Другие**, выберите виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить.

   Виджет отображается на вкладке **Панель мониторинга**. По умолчанию на виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на виджете и изменить параметры виджета, чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

   Список уведомлений на виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание ( ), защита ( ), обновления ( ), управление устройствами ( ), Защита от эксплойтов ( ), Сервер администрирования ( ).

- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.

- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** в разделе **Мониторинг**.

О статусах устройства

Kaspersky EDR Expert присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky EDR Expert учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky EDR Expert не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.

- *Предупреждение* или *Предупреждение/Видим в сети*.

- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Время, прошедшее с момента перезапуска	Устройство видимо в сети, но перезапуск требуется приложением уже дольше указанного интервала времени.	Более чем 0 минут.
Причина перезапуска	Устройство видимо в сети, но приложению требуется перезагрузка устройства по одной из выбранных причин.	• Неизвестная причина • Приложение неработоспособно до перезагрузки • Для завершения обновления требуется перезагрузка; приложение работоспособно • Для инициации обновления требуется перезагрузка • Для завершения проверки или лечения требуется перезагрузка • Требуется перезагрузка для завершения удаленной установки или удаления • Завершение шифрования данных на диске
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Менее чем 0 дней.

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Kaspersky EDR Expert позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3** дней клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Когда Kaspersky EDR Expert присваивает устройству статус, для некоторых условий (см. столбец "Описание условий" в таблице выше) учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:

   - Выберите имя группы администрирования.

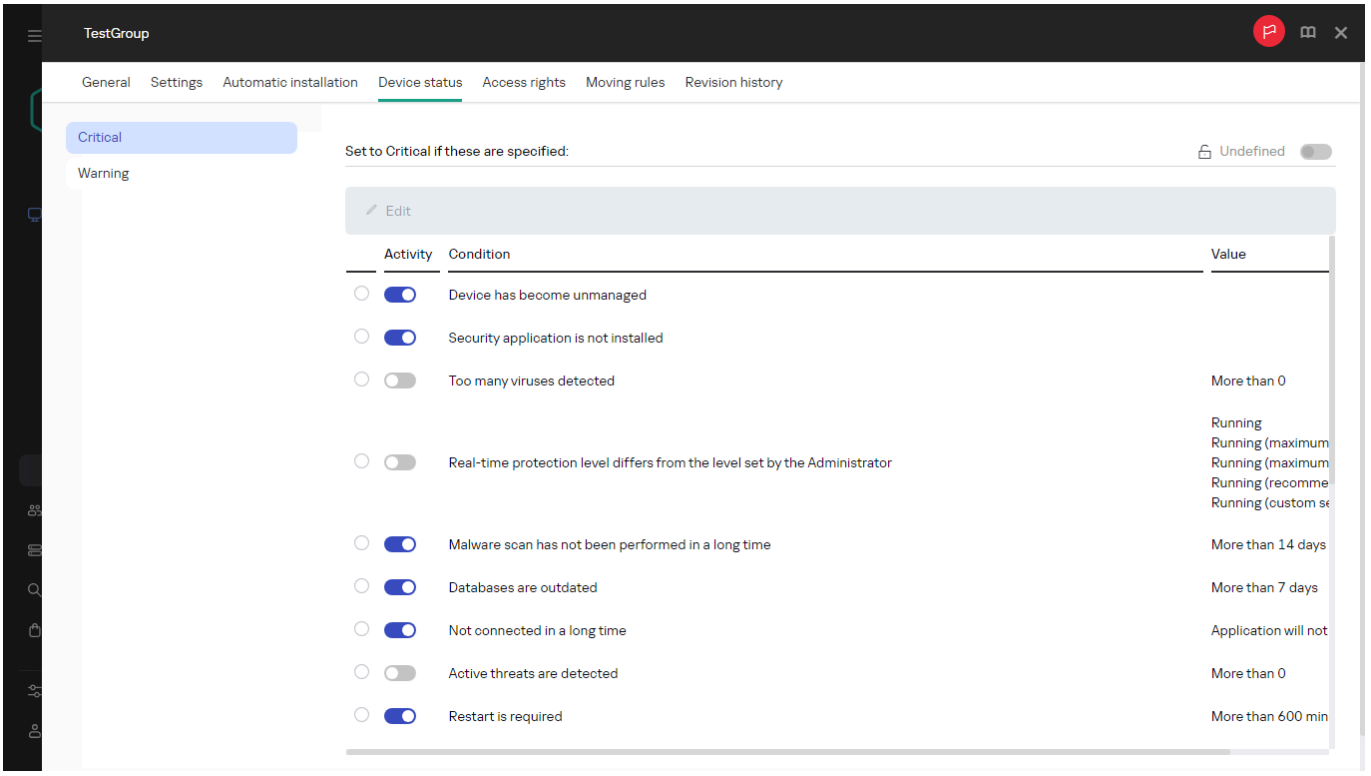
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.

3. В окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Критический**.

5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



> Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.

3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Предупреждение**.

5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Kaspersky EDR Expert. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события приложение Kaspersky EDR Expert посылает уведомление на указанные адреса электронной почты.

- SMS – при возникновении события приложение Kaspersky EDR Expert посылает уведомления на указанные номера телефонов.

- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky EDR Expert:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и на правой панели выберите вкладку с требуемым способом уведомления:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес;
     - DNS-имя SMTP-сервера.

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

     Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

     > Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

     Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

     Вы можете указать параметры подключения TLS для SMTP-сервера:

     - **Не использовать TLS**

     Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

     - **Использовать TLS, если поддерживается SMTP-сервером**

     Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

     - **Всегда использовать TLS, для проверки срока действия сертификата сервера**

     Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

     > Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky EDR Expert проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky EDR Expert не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

По нажатию на кнопку **Отправить тестовое сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **Тема** укажите тему электронной почты, используя подстановочные параметры, например: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Пример отображения темы письма в случае обнаружения угрозы: `[KSC-SAMARA-1] [Critical] Threat detected`. Также вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

Пример заполнения поля

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%
```

```
Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

Строка `Sender` является необязательной. Например, если у вас несколько Серверов администрирования, вы можете указать в качестве значения имя Сервера администрирования, с которого поступило уведомление: `Sender - KSC-SAMARA-1`.

Пример отображения текста уведомления:

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

> Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- **SMS**

  На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

  В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес;
  - Имя устройства в сети Windows (NetBIOS-имя);
  - DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

> Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать файл сертификата SMTP-сервера, перейдя по ссылке **Задать сертификаты**:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky EDR Expert проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky EDR Expert не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

> Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Исполняемый файл должен содержать переменные среды события, которые нужно передать администратору.

  В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится.

  Пример заполнения поля:

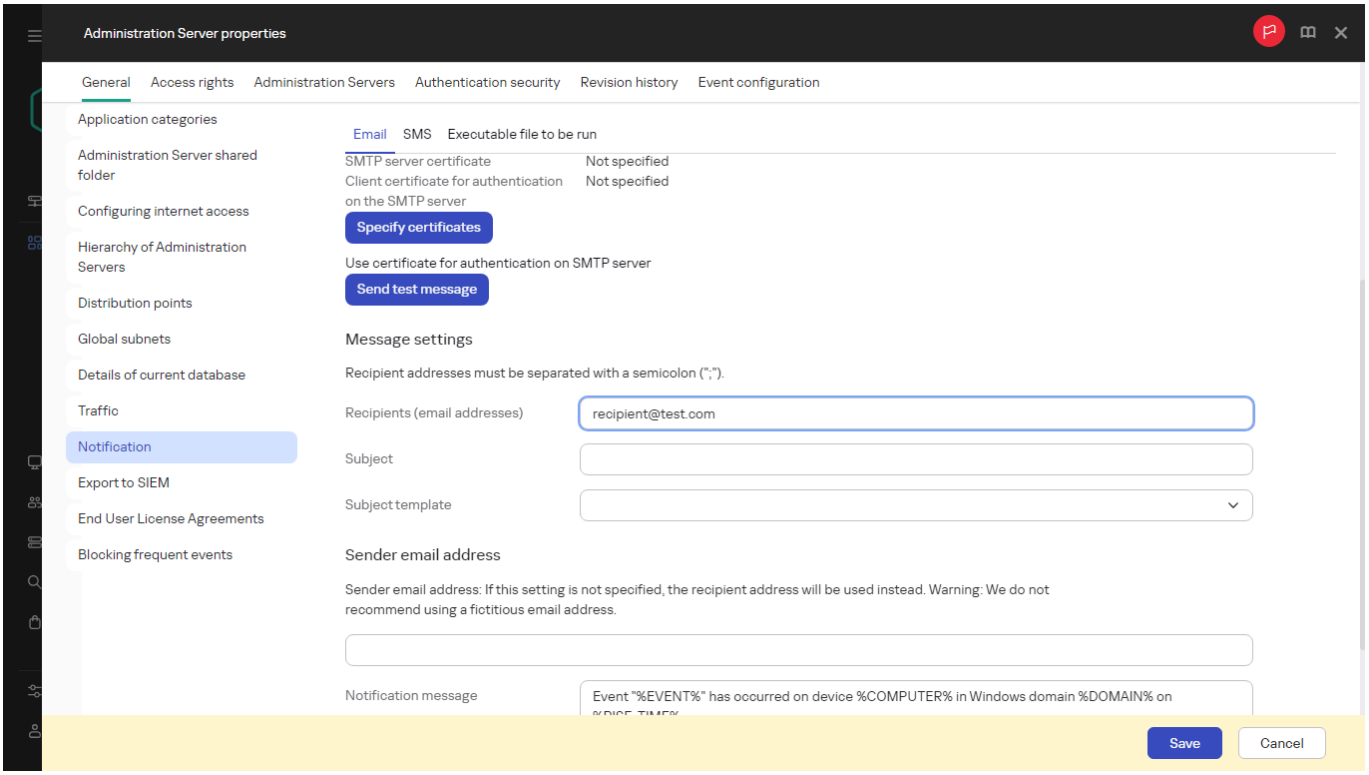
  ```
  /opt/scripts/notifications.sh
  ```

  Файл необходимо подготовить заранее, указав в нем подстановочные параметры, определяющие сведения о событии, которые будут отправлены в сообщении. Папка и файл должны находиться на Сервере администрирования.

  Пример скрипта для тестов или отладки:

  ```
  #!/usr/bin/env bash
  touch /tmp/ksc_notification.txt
  echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
  ```

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.



3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения и закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky EDR Expert.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Затем снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с тестовым "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

Чтобы открыть запись об обнаружении тестового "вируса":

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.

2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

Параметры и переменные среды для описания события

При настройке уведомлений о событиях, возникающих в Kaspersky EDR Expert, вы можете использовать для их описания параметры и переменные среды (см. таблицу ниже).

Если в качестве способа уведомления вы выбрали запуск исполняемого файла, используйте переменные при написании файла.

Если вы хотите отправлять уведомления о событиях по электронной почте или SMS, при настройке уведомлений на соответствующей вкладке вы также можете указать переменные в полях **Тема** и **Текст уведомления**.

Параметры и переменные среды для описания события

Параметр подстановки (для использования в уведомлениях)	Переменная среды (для использования в скриптах)	Описание переменной среды
%SEVERITY%	$SEVERITY	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Сбой** • **Критическое**
%COMPUTER%	$COMPUTER	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	$DOMAIN	Имя домена устройства, на котором произошло событие.
%EVENT%	$EVENT	Имя типа события. Максимальная длина названия типа события равна 50 символов.
%DESCR%	$DESCR	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	$RISE_TIME	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	$KL_PRODUCT	Название приложения.
%KL_VERSION%	$KL_VERSION	Номер версии приложения.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.
%HOST_IP%	$HOST_IP	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	$HOST_CONN_IP	IP-адрес соединения устройства, на котором произошло событие.

Мониторинг источников событий

В этом разделе представлена информация о мониторинге источников событий.

Состояние источников

В KUMA можно контролировать состояние источников, из которых поступают данные в коллекторы. На одном сервере может быть несколько источников событий, а данные из нескольких источников могут поступать в один коллектор.

Вы можете настроить автоматическое определение источников событий с помощью одного из следующих наборов полей:

- Пользовательский набор полей. Вы можете указать от 1 до 9 полей в нужной последовательности. TenantID не нужно указывать отдельно, значение определяется автоматически.

- **Применить сопоставление по умолчанию**: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Порядок полей изменить невозможно.

  Определение источников происходит, если следующие поля в событиях содержат непустые значения: DeviceProduct, DeviceAddress и/или DeviceHostname и TenantID (вам не нужно задавать значение поля TenantID, оно определяется автоматически). Поле DeviceProcessName может быть пустым. Если поле DeviceProcessName не пусто, а остальные обязательные поля заполнены, определяется новый источник.

Определение источников событий в зависимости от непустых значений в полях событий

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (определяется автоматически)	
+	+			+	Источник 1 определен
+		+		+	Источник 2 определен
+	+	+		+	Источник 3 определен
+	+		+	+	Источник 4 определен
+		+	+	+	Источник 5 определен
+	+	+	+	+	Источник 6 определен
	+	+		+	Источник не определен
	+		+	+	Источник не определен
		+	+	+	Источник не определен
+			+	+	Источник не определен

Для всей установки применяется только один набор полей. При обновлении до новой версии KUMA применяется набор полей по умолчанию. Только пользователь с ролью Главный администратор может настроить набор полей для определения источника события. После того как изменения в наборе полей сохранены, ранее определенные источники событий удаляются из Консоли KUMA и из базы данных. При необходимости вы можете вернуться к использованию набора полей для определения источников событий по умолчанию. Чтобы измененные параметры вступили в силу и приложение KUMA начала определять источники на основе новых параметров, необходимо перезапустить коллекторы.

Чтобы определить источники событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояния источников**.

2. В открывшемся окне **Состояния источников** нажмите на кнопку **Параметры**.

3. В открывшемся окне **Параметры обнаружения источника события** в раскрывающемся списке **Группирующие поля для обнаружения источников** выберите поля событий, по которым вы хотите определять источники событий.

Вы можете указать от 1 до 9 полей в нужной последовательности. В пользовательской конфигурации KUMA определяет источники, в которых заполнено поле TenantID (вам не нужно задавать значение поля, оно определяется автоматически) и заполнено хотя бы одно поле из **Группирующие поля для определения источников**. Для числовых полей 0 считается пустым значением. Если для определения источника выбрано одно числовое поле, а значение числового поля равно 0, источник не обнаруживается.

После того как вы сохранили измененный набор полей, создается событие аудита и все ранее определенные источники удаляются из Консоли KUMA и из базы данных, а примененные политики становятся неактивными.

4. Если вы хотите вернуться к списку полей для определения источника событий по умолчанию, нажмите **Применить сопоставление по умолчанию**. Порядок полей по умолчанию изменить невозможно. Если вы вручную укажете неправильный порядок полей, отобразится ошибка и кнопка сохранения параметров станет недоступной. Правильная последовательность полей по умолчанию: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Минимальная конфигурация для определения источников событий с использованием набора событий по умолчанию: непустые значения в полях DeviceProduct, DeviceAddress и/или DeviceHostName, и в поле TenantID (TenantID определяется автоматически).

5. Нажмите на кнопку **Сохранить**.

6. Перезапустите коллекторы, чтобы применить изменения и начать определение источников событий по заданному списку полей.

Определение источника настроено.

Чтобы просмотреть события, связанные с источником событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояния источников**.

   Откроется окно **Состояние источников**.

2. На вкладке **Источники событий** выберите источник события в списке. В столбце **Имя** в раскрывающемся списке для выбранного источника события выберите **События за <количество> дней**.

   KUMA выполнит переход в раздел **События**, где вы сможете просмотреть список событий для выбранного источника за последние 5 минут. Значения полей, заданные в параметрах определения источника событий, автоматически указываются в запросе. При необходимости в разделе **События** вы можете изменить период времени в запросе и снова нажать **Запустить запрос**, чтобы просмотреть данные за указанный период времени.

Ограничения

1. В конфигурации с установленным полем по умолчанию KUMA регистрирует источник события, только если необработанное событие содержит поле DeviceProduct и поля DeviceAddress и/или DeviceHostName.

Если сырое событие не содержит поля DeviceProduct и DeviceAddress и/или DeviceHostName, вы можете:

- Настроить обогащение в нормализаторе: на вкладке нормализатора **Обогащение** выберите тип данных **Событие**, укажите значение **Поле источника**, для поля **Целевое поле** выберите DeviceProduct + DeviceAddress и/или DeviceHostName и нажмите на кнопку OK.

- Использовать правило обогащения: выберите тип источника данных **Событие**, укажите значения для параметра **Исходное поле**, для параметра **Целевое поле** выберите DeviceProduct + DeviceAddress и\или DeviceHostName и нажмите **Создать**. Созданное правило обогащения необходимо привязать к коллектору на шаге Обогащение событий.

KUMA выполнит обогащение и зарегистрирует источник событий.

2. Если в KUMA поступают события с одинаковыми значениями, которые определяют источник, KUMA регистрирует разные источники при следующих условиях:

   - Значения обязательных полей совпадают, но для событий определяются разные тенанты.

   - Значения обязательных полей совпадают, но для одного из событий указано необязательное поле DeviceProcessName.

   - Значения обязательных полей совпадают, но у данных в этих полях не совпадает регистр.

Если вы хотите, чтобы KUMA регистрировала для таких событий один источник, вы можете дополнительно настроить поля в нормализаторе.

Списки источников формируются в коллекторах, объединяются в Ядре KUMA и отображаются в веб-интерфейсе приложения в разделе **Состояние источников** на вкладке **Список источников событий**. Данные обновляются ежеминутно.

Данные о частоте и количестве поступающих событий являются важным показателем состояния наблюдаемой системы. Вы можете настроить политики мониторинга, чтобы изменения отслеживались автоматически и при достижении индикаторами определенных граничных значений автоматически создавались уведомления. Политики мониторинга отображаются в Консоли KUMA в разделе **Мониторинг** → **Состояние источников** на вкладке **Политики мониторинга**.

При срабатывании политик мониторинга создаются события мониторинга с данными об источнике событий.

Список источников событий

Источники событий отображаются в таблице в разделе **Мониторинг** → **Состояние источников** → **Источники событий**. На одной странице отображается до 250 источников. Таблицу можно сортировать, нажав на заголовок столбца нужного параметра, выбрав **По возрастанию** или **По убыванию**.

Источники событий можно искать по названию с помощью поля **Поиск**. Поиск осуществляется с помощью регулярных выражений (RE2). Вы также можете фильтровать таблицу по столбцам **Статус** или **Политика мониторинга**, нажав на заголовок необходимого столбца и выбрав значения, которые вы хотите отобразить.

При необходимости вы можете настроить период обновления данных в таблице. Доступные периоды обновления: **1 минута**, **5 минут**, **15 минут**, **30 минут**, **1 час**. По умолчанию указано значение: **Не обновлять**. Настройка периода обновления может потребоваться для отслеживания изменений в списке источников.

Просмотр информации об источниках событий

На вкладке **Источники событий** информация об источниках событий отображается в следующих столбцах:

- **Статус** – статус источника:

  - зеленый – события поступают в пределах назначенных политик мониторинга;

  - красный – частота или количество поступающих событий выходит за границы, определенные хотя бы в одной в назначенной политике мониторинга;

  - серый – источнику событий не назначены политики мониторинга.

  В случае красного статуса генерируется событие типа Monitoring. Событие мониторинга формируется в тенанте, которому принадлежит источник события, и направляется в хранилище тенанта Main (хранилище должно быть предварительно развернуто в тенанте Main). Если у вас есть доступ к тенанту источника событий и нет доступа к тенанту Main, вы все равно можете осуществлять поиск по событиям мониторинга в хранилище тенанта Main, события мониторинга доступных вам тенантов будут отображаться. Также доступна отправка уведомлений по произвольному адресу электронной почты.

  Таблицу можно фильтровать по статусу.

- **Название** – название источника события. Имя формируется автоматически из значений полей, заданных в параметрах определения источника событий.

  Вы можете изменить название источника событий в таблице источников событий, наведя курсор мыши на нужное название и нажав на значок карандаша ✎. Название может содержать не более 128 символов Юникода.

- **Имя устройства или IP-адрес** – имя или IP-адрес устройства, с которого происходят события, если в параметрах определения источника событий указаны поля DeviceHostName или DeviceAddress.

- **Политика мониторинга** – список политик мониторинга, назначенных источнику событий.

  Если вы хотите отфильтровать список источников событий по примененными политикам мониторинга, нажмите на название этого столбца и выберите одну или несколько политик мониторинга. При необходимости вы можете найти нужные политики в списке с помощью поля **Поиск**.

  Вы можете просмотреть информацию обо всех политиках мониторинга, назначенных источнику событий, нажав на строку необходимого источника. В открывшемся окне отображаются параметры политик мониторинга, а также статус источника для каждой политики. Если источнику назначено несколько политик мониторинга, в случае отображения красного статуса в таблице источников в этом окне вы можете определить, какая из политик сработала. Вы также можете просмотреть, какие политики включены, а какие выключены и когда выключенные политики будут снова включены.

- **Поток** – частота, с которой из источника поступают события. Если источнику назначены политики мониторинга только типа **byCount** или политики мониторинга разных типов, поток отображается как количество событий. Если источнику назначены политики мониторинга только типа **byEPS** или политики не назначены, поток отображается как количество событий в секунду.

- **Тенант** – тенант, к которому относятся события, поступающие из источника.

Управление источниками событий

Вы можете выбрать один или несколько источников событий, установив флажки в первом столбце таблицы. Вы можете выбрать сразу несколько источников событий для выполнения групповых операций, установив флажок в первом столбце в заголовке таблицы и выбрав **Выбрать все** или **Выбрать все на странице**. Вариант **Выбрать все на странице** работает только с отображаемыми в списке источниками событий: если в списке отображаются только 500 из 1500 источников, то групповые действия по выгрузке, включению или выключению политик или удалению будут применены только к выбранным 500 источникам. Если вы хотите выполнить действие со всеми источниками в таблице, выберите **Выбрать все**.

Если выбрать источники событий, становятся доступны следующие кнопки:

- **Включение политики** – с помощью этой кнопки для источников событий можно включить политику мониторинга. Вам нужно выбрать политики мониторинга в открывшемся окне, чтобы применить их.

- **Отключить политику** – с помощью этой кнопки для источников событий можно отключить политику мониторинга. При выключении требуется указать, на какой период необходимо отключить политику: временно или навсегда.

- **Обновить политику** – с помощью этой кнопки можно применить к источникам событий включенные для них политики мониторинга или изменения уже назначенных на них политик мониторинга. При обновлении политики запускается задача в диспетчере задач.

  Эта кнопка становится доступна после того, как вы измените политики мониторинга, назначенные источникам событий.

- **Удалить** – с помощью этой кнопки источники событий можно удалить из таблицы. Статистика по этому источнику также будет удалена. Если данные из источника продолжают поступать в коллектор, источник событий снова появится в таблице, при этом его старая статистика учитываться не будет.

  Если вы хотите удалить все источники событий, но с последнего обновления таблицы прошло некоторое время, добавленные за это время источники могут не отобразится в таблице, но они будут удалены.

  Если вы удаляете более 100 000 источников событий, к которым применен фильтр или поиск, будут удалены только первые 100 000 источников событий. Вы можете снова выбрать все отфильтрованные источники событий и удалить их, а затем повторить это действие, пока не будут удалены все необходимые источники событий. Вы можете удалить более 100 000 источников событий, если к ним не применены фильтр или поиск, выбрав источники с помощью кнопки **Выбрать все**.

- **CSV** – с помощью этой кнопки можно выгрузить данные выбранных источников событий в файл CSV.

  Выгрузка поля `Stream` выполняется только если источнику события была назначена политика мониторинга, тогда в выгружаемом файле будет указана единица измерения потока, указанная в политике. Если политика не назначена, поле `Stream` пустое.

- **Диаграмма** – с помощью этой кнопки можно построить диаграмму поступления событий за последние семь дней для выбранных источников событий. Вы можете выбрать не более пяти источников событий
  .

Скачивание данных об источниках событий в файл CSV

Вы можете скачать информацию об одном или нескольких источниках событий и примененных к ним политик мониторинга в файл CSV в кодировке UTF-8. Если к источнику применены несколько политик мониторинга, в файле для этого источника каждая политика мониторинга и ее параметры будут записаны на отдельной строке. Для каждой политики мониторинга, примененной к источнику, в файл будут выгружены следующие параметры: **Статус**, **Название**, **Политика мониторинга**, **Нижний порог**, **Верхний порог**, **Поток**, **Тенант**.

Чтобы скачать информацию об источниках событий в файл CSV:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Источники событий** выберите в таблице один или несколько источников событий, установив флажки в первом столбце напротив нужных источников.

   В левой нижней части таблицы отображается количество выбранных источников и общее количество источников в таблице. Вы можете выбрать не более 150 000 источников событий.

   Вы можете выбрать сразу несколько источников событий в списке, установив флажок в первом столбце в заголовке таблицы и выбрав одно из следующих значений:

   - **Выбрать все** – выбрать все источники событий на всех страницах таблицы. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники, удовлетворяющие условию поиска.
   - **Выбрать все на странице** – выбрать все источники событий на открытой странице. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники на открытой странице, удовлетворяющие условию поиска.

2. Нажмите на кнопку **CSV** со значком плюса в верхней части таблицы.

   > В зависимости от размера окна вашего браузера кнопка **CSV** может находиться в дополнительном меню, доступном при нажатии на значок в виде трех точек ⋮.

   Новая задача экспорта источников событий будет создана в диспетчере задач.

3. Перейдите в раздел **Диспетчер задач** и найдите созданную задачу в списке задач.

   Когда файл будет готов, в строке задачи в столбце **Статус** отобразится статус **Завершено**.

4. Нажмите на название типа задачи и в раскрывающемся списке выберите пункт **Скачать**.

CSV-файл с информацией об источниках будет скачан с использованием параметров вашего браузера. Имя файла по умолчанию event-source-list.csv.

Просмотр динамики поступления событий

Вы можете изучить динамику поступления событий от источника за последние семь дней с учетом примененных политик мониторинга одним из следующих способов:

- Просмотреть график для одного источника событий.
- Построить диаграмму на основе графиков для нескольких источников (не более пяти).

Чтобы просмотреть граф для отдельного источника событий, перейдите в раздел **Мониторинг** → **Состояние источников** → **Источники событий** и нажмите на значок стрелки › в строке соответствующего источника событий. График поступления событий откроется под строкой источника.

Данные на графике отображаются следующим образом:

- Данные отображаются за те дни, в которые поступали события. Максимальный период – семь дней.

  В левом верхнем углу над графиком вы можете просмотреть количество дней, а в правом верхнем углу – период отображение данных. Вы можете нажать на кнопку **События за <количество> дней**, чтобы перейти в раздел **События** и просмотреть список событий для выбранного источника.

- На оси X отображаются дни, на оси Y – частота поступления событий (EPS).

- Линии отражают среднее, максимальное и минимальное количество событий за каждые 15 минут в течение последних семи дней.

  Если вы хотите просмотреть количество событий в конкретное время, наведите курсор мыши на точку на графике. Отобразится всплывающая подсказка со средним, максимальным и минимальным количеством событий на конкретные дату и время.

Вы также можете построить диаграмму поступления событий на основе графиков для нескольких источников событий, например, если вам нужно сравнить активность однотипных источников событий, которые должны вести себя похоже, но фактически ведут себя по-разному.

Чтобы построить диаграмму на основе графиков для нескольких источников событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Источники событий** выберите в таблице один или несколько источников событий, установив в первом столбце флажки рядом с нужными источниками.

   Вы можете построить диаграмму максимум для 5 источников событий одновременно.

2. Нажмите на кнопку **Диаграмма** в верхней части таблицы.

   > В зависимости от размера окна вашего браузера кнопка **Диаграмма** может находиться в дополнительном меню, доступном при нажатии на значок в виде трех точек ⋮.

   В открывшейся панели **Диаграмма** отобразится диаграмма поступления событий для всех выбранных источников, а также таблица, в которой для каждого источника отображается текущее количество событий, максимальное и среднее количество событий, рассчитанные по данным на диаграмме. Вы можете сравнить, как данные для выбранных источников соотносятся друг с другом во времени.

   Данные на диаграмме отображаются следующим образом:

   - Данные отображаются за те дни, в которые поступали события. Максимальный период – семь дней.

     В правом верхнем углу над диаграммой вы можете просмотреть период отображение данных.

   - На оси X отображаются дни, на оси Y – частота поступления событий (EPS).

   - Линии на диаграмме отображают среднее количество поступивших событий для выбранных источников событий за каждые 15 минут в течение последних семи дней.

   Вы можете навести курсор мыши на диаграмму, чтобы просмотреть среднее количество событий для каждого источника в конкретное время.

3. При необходимости снимите флажки в таблице под диаграммой напротив тех источников событий, которые вы хотите скрыть на диаграмме.

4. Если вы хотите отобразить диаграмму более детализированно, нажмите на значок двух стрелок ↙↗, чтобы открыть панель на весь экран и увеличить масштаб диаграммы.

Политики мониторинга

Данные о частоте и количестве поступающих событий являются показателем состояния системы. Например, можно обнаружить, когда поток событий стал аномально большим, слишком слабым или вообще прекратился. Политики мониторинга предназначены для отслеживания таких ситуаций. В политике вы можете задать нижнее пороговое значение, дополнительно задать верхний порог, и каким образом будут считаться события: по частоте или по количеству.

Политику нужно применить к источнику события. Вы можете применить к источнику одну или несколько политик мониторинга. После применения политики вы можете отслеживать статус источника на вкладке **Список источников событий**.

Политики мониторинга источников событий отображаются в таблице в разделе **Мониторинг** → **Состояние источников** → **Политики мониторинга**. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. Максимальный размер списка политик не ограничен.

В столбце **Источники** вы можете нажать на кнопку **Показать**, чтобы просмотреть все источники событий, к которым применена политика. При нажатии на эту кнопку вы будете перенаправлены на вкладку **Источники событий**, и таблица источников будет отфильтрована по выбранной политике.

Алгоритм работы политик мониторинга

Политики мониторинга применяются к источнику события по следующему алгоритму:

1. Поток событий подсчитывается на коллекторе.

2. Сервер Ядра KUMA с интервалом в 15 секунд собирает с коллекторов информацию о потоке.

3. Собранные данные хранятся на сервере Ядра KUMA в СУБД временных рядов VictoriaMetrics, и срок хранения данных на сервере Ядра KUMA составляет 15 суток.

4. Инвентаризация источников событий выполняется один раз в минуту.

5. Поток подсчитывается отдельно для каждого источника событий по следующим правилам:

   - Если к источнику событий применяется политика мониторинга, то максимальное число потока событий считается согласно работающим в текущий момент политикам мониторинга за интервал времени, указанный в политике.

     В зависимости от типа политики число потока событий подсчитывается как количество событий (для типа политики **byCount**) или как количество событий в секунду (EPS, для политики типа **byEPS**). Вы можете узнать, в чем считается поток для назначенной политики, в столбце **Поток** на вкладке **Источники событий**.

   - Если к источнику событий не применяется политика мониторинга, число потока событий отображает последнее значение.

6. Один раз в минуту проверяется, есть ли политики мониторинга, которые должны примениться к источникам событий или остановиться в соответствии с расписанием политики мониторинга.

7. Поток событий проверяется на соответствие параметрам политики один раз в минуту.

Если поток событий от источника выходит за пределы значений, указанных в политике мониторинга, информация об этом будет зафиксирована следующим образом:

- Уведомление о срабатывании политики мониторинга будет отправлено на адреса электронной почты, указанные в политике. Для каждой политики вы также можете задать шаблон уведомления.

- Будет сформировано информационное событие мониторинга потоков типа `5` (`Type=5`). Поля события описаны в таблице ниже.

Поля события мониторинга

Название поля события	Значение поля
ID	Уникальный идентификатор события.
Timestamp	Время события.
Тип.	Тип события аудита. Событию аудита соответствует значение `5` (мониторинг).
Имя	Название политики мониторинга.
DeviceProduct	`KUMA`
DeviceCustomString1	Значение из поля `value` в уведомлении. Отображается значение метрики, по которой отправлено уведомление.

Сформированное событие мониторинга будет отправлено в следующие ресурсы:

- все хранилища тенанта Main;

- все корреляторы тенанта Main;

- все корреляторы тенанта, в котором находится источник событий.

Добавление политики мониторинга

Чтобы добавить новую политику мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Политики мониторинга**, нажмите **Добавить политику** и в открывшемся окне укажите параметры политики мониторинга.

2. В поле **Название политики** введите уникальное имя создаваемой политики. Название должно содержать от 1 до 128 символов Юникода.

   Рекомендуется отразить расписание работы политики мониторинга, которое вы настроили в параметрах, в названии политики.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать политика. От выбора тенанта зависит, для каких источников событий можно будет включить политику мониторинга.

4. В поле **Тип** выберите один из следующих вариантов типа политики мониторинга:

   - **количество поступивших событий** – по количеству событий за определенный промежуток времени.

   - **Частота поступления событий** – по количеству событий в секунду за определенный промежуток времени (EPS). Считается среднее значение за весь промежуток. Можно дополнительно отслеживать скачки в определенные периоды.

5. В поле **Период подсчета** укажите, за какой период в политике мониторинга должны учитываться данные из источника мониторинга. Вы можете выбрать значение в минутах, часах или днях с помощью раскрывающегося списка справа. Максимальное значение: 14 дней.

6. Если вы выбрали тип политики **частота поступления событий**, в поле **Регулярность замеров, мин** укажите контрольный интервал времени в минутах, в течение которого проверки должны фиксировать отклонение числа потока событий от нормы для срабатывания политики мониторинга:

   - Если в течение этого времени все проверки, проводимые один раз в минуту, зафиксировали отклонение потока от нормы, сработает политика мониторинга.

   - Если в течение этого времени одна из проверок, проводимых один раз в минуту, зафиксировала, что поток соответствует норме, политика мониторинга не сработает и подсчет результатов проверок начнется заново.

   Если вы не укажете регулярность замеров, политика мониторинга сработает сразу после того, как будет зафиксировано отклонение потока от нормы.

7. В полях **Нижний порог** и **Верхний порог** определите, выход за какие границы будет считаться отклонением от нормы. Отклонения от этих значений активируют политику мониторинга, которая создает алерты и пересылает уведомления.

   Параметр **Нижний порог** является обязательным.

8. В поле **Интервал оценки** укажите частоту, с которой сервис VMalert будет делать запрос в VictoriaMetrics на получение данных по политике, пока она применяется к источнику событий. Вы можете выбрать значение в минутах, часах или днях с помощью раскрывающегося списка справа. По умолчанию интервал составляет 5 минут.

   При указании интервала оценки учитывайте расписание применения политики. Например, если вы указали применение политики ежедневно раз в несколько часов, не рекомендуется устанавливать частый интервал оценки, чтобы не перегружать VictoriaMetrics.

9. При необходимости в поле **Отправлять уведомления** укажите электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA. Для добавления каждого адреса введите его в поле и нажмите **`Enter`** или **Добавить**. Можно указать несколько адресов электронной почты.

   Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу.

10. В раскрывающемся списке **Шаблон уведомлений** выберите шаблон, который будет использоваться для уведомлений. При необходимости нажмите на кнопку **Создать**, чтобы перейти к созданию нового шаблона уведомления.

    По умолчанию выбран базовый шаблон уведомлений. Вы можете сбросить выбранный шаблон и переключиться на базовый шаблон, нажав на значок крестика.

11. В разделе параметров **Расписание** настройте период применения политики мониторинга к источникам событий. По умолчанию политика применяется еженедельно каждый день с 00:00 до 23:59. Для настройки расписания применения политики мониторинга выполните одно или несколько следующих действий:

    - Если вы хотите применять политику мониторинга еженедельно в конкретные дни недели:

      a. Включите переключатель **Настроить расписание по дням недели**.

      b. В раскрывающемся списке **Дни недели** выберите дни недели, в которые политика будет применяться к источнику.

      Если вы хотите очистить выбор, нажмите на значок крестика.

      c. В поле **Время** укажите время начала и окончания работы политики с точностью до минуты.

      Границы указанного периода включаются, например, если время окончания применения политики указано 23:59, политика будет работать до 23:59:59.999. По умолчанию указано время с 00:00 до 23:59. Время начала должно быть меньше времени окончания.

      d. Если вы хотите добавить еще один период срабатывания политики, нажмите на кнопку **Добавить период** и повторите шаги b и c.

      Вы можете добавить неограниченное количество периодов.

    - Если вы хотите применять политику мониторинга в конкретные календарные дни:

      a. Включите переключатель **Настроить расписание по конкретным дням**.

      b. Нажмите на поле **Дни месяца** и выберите в календаре дни, в которые политика будет применяться к источнику. Вы можете выбрать период в несколько дней или только один день. Дата начала периода должна быть меньше даты окончания периода.

      Дни не привязаны к году, поэтому политика будет применяться ежегодно в указанные дни, пока вы не удалите этот период. Если вы хотите очистить выбор, нажмите на значок крестика.

      c. В поле **Время** укажите время начала и окончания работы политики с точностью до минуты.

      Границы указанного периода включаются, например, если время окончания применения политики указано 23:59, политика будет работать до 23:59:59.999. По умолчанию указано время с 00:00 до 23:59. Время начала должно быть меньше времени окончания.

      d. Если вы хотите добавить еще один период срабатывания политики, нажмите на кнопку **Добавить период** и повторите шаги b и c.

      Вы можете добавить неограниченное количество периодов.

    Если вы применили расписание по дням недели и по конкретным дням месяца одновременно, то в первую очередь применяется политика по дням месяца.

12. Нажмите на кнопку **Добавить**.

Политика мониторинга добавлена.

Изменение политики мониторинга

В разделе **Мониторинг** → **Состояние источников** → **Политики мониторинга** отображаются добавленные политики мониторинга и их параметры, которые вы задали при создании политики. Вы можете нажать на политику, чтобы просмотреть все параметры этой политики в открывшейся боковой панели. При необходимости в этой панели вы можете изменить параметры политики.

Если политика мониторинга применена к источнику событий, при изменении некоторых параметров политики может потребоваться ее обновить, чтобы применить изменения. Каждые 30 минут KUMA проверяет, есть ли политики мониторинга, требующие обновления, и при наличии таких политик автоматически запускает задачу обновления этих политик мониторинга. Вы также можете запустить задачу обновления вручную, нажав на кнопку **Обновить политику** в верхней части таблицы. Все политики, которые требуют обновления, будут обновлены в рамках одной задачи.

Кнопка **Обновить политику** становится активна, только если есть политики мониторинга, требующие обновления. Информация о необходимости обновления политики отображается в таблице политик мониторинга в столбце **Статус обновления политики** в виде одного из следующих статусов:

- **Требуется обновить** – один из следующих параметров политики мониторинга был изменен, но изменения не были применены к источникам событиям:
  - **Название политики**
  - **Тип**
  - **Нижний порог**
  - **Верхний порог**
  - **Период подсчета**
  - **Регулярность замеров**
  - **Интервал оценки**
- **Обновлена** – отображается в одном из следующих случаев:
  - После изменения политики запускалась задача применения политики и изменения были применены к источникам событий.
  - Вы изменили один из следующих параметров политики, который не требует запуска задачи обновления:
    - **Отправлять уведомления**
    - **Шаблон уведомлений**
    - **Расписание**

    В этом случае измененные параметры политики будут применены к источникам событий через минуту. Изменения в параметре **Шаблон уведомлений** применяются сразу.
  - Измененная политика мониторинга не применяется к источникам событий.

Дата и время, когда политика последний раз была применена к источникам событий, отображаются в столбце **Дата последнего применения политики**.

> Пока запущена задача обновления политики, кнопка **Обновить политику** недоступна для всех пользователей. Если другой пользователь изменил параметры политики, требующие ее обновления, кнопка **Обновить политику** будет активна для вас только после того, как вы обновите страницу или измените политику или источник событий.

Применение политики мониторинга

Чтобы применить политики мониторинга к источникам событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Источники событий** выберите в таблице один или несколько источников событий, установив флажки в первом столбце рядом с нужными источниками. Вы можете выбрать сразу несколько источников событий в списке, установив флажок в первом столбце в заголовке таблицы и выбрав одно из следующих значений:

   - **Выбрать все** – выбрать все источники событий на всех страницах таблицы. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники, удовлетворяющие условию поиска.

   - **Выбрать все на странице** – выбрать все источники событий, прогрузившиеся на открытой странице. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники на открытой странице, удовлетворяющие условию поиска.

   В левой нижней части таблицы отображается количество выбранных источников и общее количество источников в таблице.

   После того как вы выберете в списке источники событий, к которым хотите применить политику мониторинга, в панели инструментов станет доступна кнопка **Включение политики**.

2. Нажмите **Включить политику**.

3. В открывшемся окне **Включить политику** выберите одну или несколько политик мониторинга, которые вы хотите применить к выбранным источникам событий. В таблице отображаются только политики мониторинга, которые вы можете назначить для выбранных источников: принадлежащие тому же тенанту или Общему тенанту, если у вас есть к нему доступ. Если для выбранных источников событий нет общих политик и у вас нет доступа к Общему тенанту, таблица политик будет пустой.

   Вы можете выбрать все доступные политики, установив флажок в первом столбце в заголовке таблицы. Вы также можете воспользоваться контекстным поиском по названию политик или отсортировать политики, нажав на заголовок столбца, по которому вы хотите отсортировать таблицу, и выбрав **По возрастанию** или **По убыванию**.

   > Поиск и сортировка недоступны для столбцов **Источники**, **Расписание**, **Статус обновления политики**, **Дата последнего применения политики**.

4. Нажмите **Применить**.

5. В таблице источников нажмите **Обновить политику**, чтобы применить изменения к источникам событий.

   Политики мониторинга применены к выбранным источникам событий, статус этих источников изменится на зеленый. Названия примененных к источникам политик отобразятся в столбце **Политика мониторинга**. Также отобразится сообщение о количестве источников, к которым были применены политики. Если политика мониторинга сработает на источнике событий, изменение статуса этого источника отобразится после того, как вы обновите страницу вручную или она обновится автоматически. Рекомендуется настроить период автоматического обновления данных для отслеживания изменений в списке источников.

Если вы выбрали более 100 000 источников событий и применили к ним одну или несколько политик, эти политики будут применены только к первым 100 000 источникам, к которым эти политики еще не были применены. Если вам нужно применить политики к оставшимся источникам, вы можете выполнить одно из следующих действий:

- Еще раз выбрать все источники и применить к ним нужные политики.
- Отфильтровать таблицу источников по какому-либо параметру таким образом, чтобы в таблице отобразилось не более 100 000 источников, и применить к ним нужные политики.

Повторите выбранное действие до тех пор, пока политики не будут применены ко всем нужным источникам.

Отключение политики мониторинга

Чтобы отключить политики мониторинга от источников событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Источники событий** выберите в таблице один или несколько источников событий, установив флажки в первом столбце рядом с нужными источниками.

   В левой нижней части таблицы отображается количество выбранных источников и общее количество источников в таблице. После того как вы выберете в списке источники событий, для которых применены политики мониторинга, в панели инструментов станет доступна кнопка **Отключить политику**.

   Вы можете выбрать сразу несколько источников событий в списке, установив флажок в первом столбце в заголовке таблицы и выбрав одно из следующих значений:

   - **Выбрать все** – выбрать все источники событий на всех страницах таблицы. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники, удовлетворяющие условию поиска.
   - **Выбрать все на странице** – выбрать все источники событий, прогрузившиеся на открытой странице. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники на открытой странице, удовлетворяющие условию поиска.

2. Нажмите **Отключить политику**.

3. В открывшемся окне **Отключить политику** выберите одну или несколько политик мониторинга, которые вы хотите отключить для выбранных источников событий. В таблице отображаются все политики мониторинга, примененные хотя бы к одному из выбранных источников событий.

   Вы можете выбрать все доступные политики, установив флажок в первом столбце в заголовке таблицы. Вы также можете воспользоваться контекстным поиском или отсортировать политики, нажав на заголовок столбца, по которому вы хотите отсортировать таблицу, и выбрав **По возрастанию** или **По убыванию**.

Поиск и сортировка недоступны для столбцов **Источники**, **Расписание**, **Статус обновления политики**, **Дата последнего применения политики**.

4. В блоке параметров над таблицей политик выполните одно из следующих действий

   - Если вы хотите временно приостановить применение политик, выберите **На определенное время** и укажите время в минутах, часах или днях, по истечении которого выбранные политики снова будут применены к источникам событий Максимальные значения:

     - для дней – 30;

     - для часов – 743;

     - для минут – 44579.

   - Если вы хотите отключить выбранные политики от источников событий навсегда, выберите **Пока не включите вручную**.

   По умолчанию выбрано **На определенное время** и установлено значение **5 минут**.

5. Нажмите **Выключить**.

6. В таблице источников нажмите **Обновить политику**, чтобы применить изменения к источникам событий.

   Политики мониторинга отключены от выбранных источников событий или приостановлены на указанное время. Статус этих источников изменится на серый в таблице. Отобразится сообщение о количестве источников, для которых были отключены политики.

Если вы выбрали более 100 000 источников событий и отключили от них одну или несколько политик, эти политики будут отключены только от первых 100 000 источников, к которым эти политики применены. Если вам нужно отключить политики от оставшихся источников, вы можете выполнить одно из следующих действий:

- Еще раз выбрать все источники и отключить для них нужные политики.

- Отфильтровать таблицу источников по какому-либо параметру таким образом, чтобы в таблице отобразилось до 100 000 источников включительно, и отключить для них нужные политики.

Повторите выбранное действие до тех пор, пока политики не будут отключены от всех нужных источников.

Добавление новой политики мониторинга на основе существующей

Чтобы создать политику мониторинга на основе существующей:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Состояние источников** → **Политики мониторинга** и выберите политику мониторинга, на основе которой вы хотите создать политику.

   При необходимости вы можете найти необходимые политики мониторинга с помощью поля **Поиск**. Поиск будет осуществляться по столбцам **Название**, **Тенант**, **Тип**, **Расписание** (день недели и время).

2. Нажмите на кнопку **Дублировать политику**.

3. В открывшемся окне **Добавить политику** измените параметры политики.

   По умолчанию в название новой политики будет добавлено `- copy`. Остальные параметры будут такие же, как в политике, на основе которой выполнялось дублирование.

4. Нажмите на кнопку **Добавить**, чтобы создать политику.

Политика мониторинга создана на основе существующей политики.

Удаление политики мониторинга

Чтобы удалить политику мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Статус источника** → **Политики мониторинга** и выберите одну или несколько политик мониторинга, которые вы хотите удалить.

   При необходимости вы можете найти необходимые политики мониторинга с помощью поля **Поиск**. Поиск будет осуществляться по столбцам **Название**, **Тенант**, **Тип**, **Расписание** (день недели и время).

2. Нажмите **Удалить политику** и подтвердите действие.

Выбранные политики мониторинга удалены.

> Невозможно удалить предустановленные политики мониторинга, а также политики, назначенные источникам событий.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

Об объявлениях "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Open Single Management Platform периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Open Single Management Platform показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

> Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

  Объявления, связанные с безопасностью, предназначены для того, чтобы приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию.

  Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при установке Сервера администрирования.

- Рекламные объявления.

  Рекламные объявления включают информацию о специальных предложениях для ваших приложений "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

  Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Предупреждение.
3. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" приложение OSMP Console отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Если вы не хотите получать объявления, вы можете отключить эту функцию.

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления.

Чтобы выключить объявления, связанные с безопасностью:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.

3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.

4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Отключение KSN может повлиять на работу управляемых приложений "Лаборатории Касперского", использующих службы KSN. Эти приложения могут утратить возможность обмена данными о репутации, телеметрией или статистикой с "Лабораторией Касперского".

Cloud Discovery

Open Single Management Platform позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Блокировать доступ можно, только если вы активировали Open Single Management Platform по лицензии Kaspersky EDR Expert.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

- Вы приобрели лицензию на Kaspersky Next, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробную информацию см. в справке Kaspersky Next.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в виджете Cloud Discovery и в отчетах Cloud Discovery. Виджет также показывает уровень риска каждого облачного сервиса. Open Single Management Platform получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности или профилями политик, в которых она включена.

Включение функции Cloud Discovery с помощью виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security for Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security for Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security for Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security for Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы включить функцию Cloud Discovery с помощью виджета Cloud Discovery:

1. Откройте Kaspersky EDR Expert.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
3. В виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security for Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security for Windows.

   Если у вас версия Kaspersky Endpoint Security for Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security for Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, виджет добавлен в панель мониторинга.

Добавление виджета Cloud Discovery в панель мониторинга

Вы можете добавить виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить виджет Cloud Discovery в панель мониторинга, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы добавить виджет Cloud Discovery в панель мониторинга:

1. Откройте Kaspersky EDR Expert.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить виджет**.
4. В списке доступных виджетов нажмите на значок шеврона (>) рядом с категорией **Другое**.
5. Выберите виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

   Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью виджета.

Выбранный виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Виджет также показывает уровень риска каждого облачного сервиса. Open Single Management Platform получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Перед просмотром убедитесь, что:

- Виджет Cloud Discovery добавлен в панель мониторинга.
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы посмотреть виджет Cloud Discovery:

1. Откройте Open Single Management Platform.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.

   Виджет **Cloud Discovery** отображается в панели мониторинга.

3. В левой части виджета **Cloud Discovery** выберите категорию облачных сервисов.

   В таблице в правой части виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.

4. В правой части виджета выберите требуемый сервис.

   В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису. В этой таблице вы можете сформировать два типа отчетов: отчет об успешных попытках доступа и отчет о заблокированных попытках доступа.

   Также в этой таблице вы можете заблокировать доступ к облачной службе для определенного устройства.

В виджете отображаются запрашиваемые данные.

В отображаемом виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису.

Блокировать доступ можно, только если вы активировали Open Single Management Platform по лицензии Kaspersky EDR Expert.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачных сервисов

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить сервисы, не соответствующие требованиям безопасности вашей организации. Например, вы можете принять во внимание уровень риска при принятии решения о блокировке доступа к определенному сервису.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в виджете Cloud Discovery и в списке всех контролируемых облачных сервисов.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security for Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security for Windows.

Чтобы заблокировать или разрешить доступ к облачному сервису с помощью виджета:

1. Откройте виджет Cloud Discovery и выберите требуемый облачный сервис.

2. В панели **Топ 10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.

3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:

   - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.

   - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.

4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

Kaspersky EDR Expert позволяет выполнять настройку экспорта событий в SIEM-системы одним из следующих способов: экспорт в любую SIEM-систему, использующую формат syslog, экспорт в Kaspersky SIEM (KUMA), QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы данных Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky EDR Expert:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что у вас есть значения системных параметров.

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- **Настройка SIEM-системы для получения событий из Kaspersky EDR Expert**

  Инструкции: Настройка экспорта событий в SIEM-системе.

- **Выбор событий, которые вы хотите экспортировать в SIEM-систему**

  Отметьте события, которые вы хотите экспортировать в SIEM-систему. Отметьте общие события, которые возникают во всех управляемых приложениях "Лаборатории Касперского". Затем можно отметить события для экспорта для определенного управляемого приложения.

- **Настройка экспорта событий в SIEM-систему**

  Экспортировать события можно следующими способами:

  - Использование протоколов TCP, UDP или TLS over TCP.
  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky EDR Expert необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky EDR Expert.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky EDR Expert и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky EDR Expert и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky EDR Expert в SIEM-систему. Это значение необходимо указать в настройках Kaspersky EDR Expert и настройках приемника в SIEM-системе.

Об экспорте событий

Kaspersky EDR Expert позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ алертов систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky EDR Expert во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky EDR Expert и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky EDR Expert. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky EDR Expert, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky EDR Expert

Существует три способа отправки событий из Kaspersky EDR Expert во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  Используя протокол Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события в OSMP Console. Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы Kaspersky SIEM, QRadar, Splunk и ArcSight

Протоколы CEF и LEEF можно использовать для экспорта общих событий. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. Для конвертации событий Open Single Management Platform в события формата CEF и LEEF используется файл siem_conversion_rules.xml. Этот файл содержит список атрибутов событий Kaspersky EDR Expert и соответствующие атрибуты событий в формате CEF и LEEF. Также файл siem_conversion_rules.xml содержит правила генерации сообщений, соответствующих событиям. Этот файл входит в комплект поставки Kaspersky EDR Expert.

В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (Kaspersky SIEM (KUMA), QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky EDR Expert в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky EDR Expert. Для этого необходимо правильно настроить SIEM-систему. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky EDR Expert во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky EDR Expert и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky EDR Expert.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky EDR Expert. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта**

  Протокол передачи сообщений UDP, TCP или TLS over TCP. Необходимо указать тот же протокол, который был выбран в Kaspersky EDR Expert для передачи событий.

- **Порт**

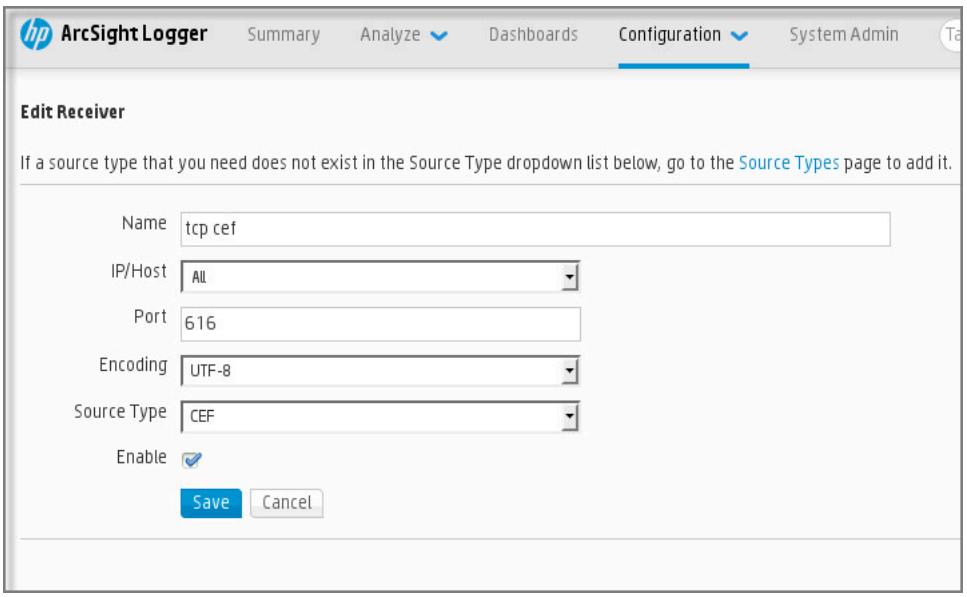
  Укажите номер порта для подключения к Kaspersky EDR Expert. Этот порт должен совпадать с портом, который вы указываете в Kaspersky EDR Expert при настройке экспорта событий в SIEM-систему.

- **Формат даты**

  Укажите формат syslog, CEF или LEEF.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.



Настройка приемника в ArcSight

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, чтобы информация о событиях могла быть использована SIEM-системой. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения содержимого сообщения на соответствующие поля, такие как код события, уровень важности, описание, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky EDR Expert, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

Выбор событий для экспорта в SIEM-системы в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

Для событий изменения политик вы можете только включить или выключить экспорт всех таких событий в SIEM-систему.

О выборе событий для экспорта в SIEM-систему в формате syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

Чтобы отметить события для экспорта для определенного управляемого приложения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите политику приложения, для которого нужно отметить события.

   Откроется окно свойств политики.

3. Перейдите в раздел **Настройка событий**.

4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемого приложения готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике приложения, вам не удастся переопределить выбранные события для управляемого устройства.

Чтобы выбрать события для управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Отобразится список управляемых устройств.

2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.

3. Перейти в раздел **Приложения**.

4. Перейдите по ссылке с названием требуемого приложения в списке приложений.

5. Перейдите в раздел **Настройка событий**.

6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

8. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Выбор общих событий для экспорта в формате Syslog

Вы можете отметить общие события, которые Сервер администрирования будет экспортировать в SIEM-системы, используя формат Syslog.

Чтобы выбрать общие события для экспорта в SIEM-систему:

1. В главном окне приложения выполните одно из следующих действий:
   - Нажмите на имя Сервера администрирования.
   - Перейдите в раздел **Управление активами** → **Политики**, а затем перейдите по ссылке политики.
2. В открывшемся окне перейдите на вкладку **Настройка событий**.
3. Нажмите **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 используется для экспорта событий из Kaspersky EDR Expert во внешние системы.

В Kaspersky EDR Expert можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky EDR Expert таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky EDR Expert начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий, событий изменения политик и событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует. Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Open Single Management Platform в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center.

- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky EDR Expert отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

Конвертация событий в формат CEF или LEEF

Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Open Single Management Platform в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml. Этот файл входит в комплект поставки Open Single Management Platform.

Файл siem_conversion_rules.xml содержит предустановленные правила интерпретации для конвертации событий в формат CEF и LEEF. Если вы хотите использовать дополнительные правила интерпретации событий, вы можете добавить их в файл вручную.

Файл siem_conversion_rules.xml включает следующие секции:

- `<product name="SP_QRADAR" vendor="IBM">`

  Эта секция содержит правила генерации событий в формате LEEF, которые можно экспортировать в SIEM-систему QRadar.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Эта секция содержит правила генерации событий в формате CEF, которые можно экспортировать в SIEM-систему ArcSight или Splunk.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Эта секция содержит правила генерации событий в формате CEF, которые можно экспортировать в KUMA.

В каждом разделе есть подраздел `<common>`, в котором размещены атрибуты событий Open Single Management Platform и соответствующие им атрибуты событий в формате LEEF. Эти общие атрибуты используются для всех типов событий, которые можно экспортировать.

Каждый раздел также имеет подраздел `<event>`. Каждый подраздел `<event>` содержит дополнительные атрибуты, которые добавляются к атрибутам, указанным в разделе `<common>`.

Вы можете вручную добавить новое правило генерации событий в файл siem_conversion_rules.xml.

Чтобы добавить новое правило генерации событий:

1. Добавьте новый подсекцию `<event>` в секцию `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` или `<product name="Kaspersky SIEM" vendor="Kaspersky">`, а затем укажите дополнительные атрибуты события, если необходимо.

2. Если событие состоит только из общих атрибутов, подраздел `<event>` будет пустым.

siem_conversion_rules.txt

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
```

```
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Настройка Kaspersky EDR Expert для экспорта событий в SIEM-систему

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky EDR Expert.

Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky EDR Expert в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Чтобы настроить экспорт в SIEM-системы из OSMP Console:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Экспорт в SIEM-систему**.

3. Перейдите по ссылке **Параметры**.

   Откроется раздел **Параметры экспорта**.

4. Укажите параметры в разделе **Параметры экспорта**:

   - **Адрес сервера SIEM-системы**

     Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

   - **Порт SIEM-системы**

     Номер порта, по которому будет установлено соединение между Kaspersky EDR Expert и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky EDR Expert и настройках приемника в SIEM-системе.

   - **Протокол**

     Выберите протокол передачи сообщений в SIEM-систему. Вы можете выбрать протокол TCP, UDP или TLS over TCP.

     Укажите следующие параметры TLS, если вы выбираете TLS over TCP:

     - **Аутентификация Сервера**

В поле **Аутентификация Сервера** можно выбрать значения **Доверенные сертификаты** или же **Отпечатки SHA**:

- **Доверенные сертификаты**. Вы можете получить полную цепочку сертификатов (включая корневой сертификат) от доверенного центра сертификации (CA) и загрузить файл в Open Single Management Platform. Open Single Management Platform проверяет, подписана ли цепочка сертификатов SIEM-системы также доверенным центром сертификации или нет.

  Чтобы добавить доверенный сертификат, нажмите на кнопку **Выбрать файл центра сертификации** и загрузите сертификат.

- **Отпечатки SHA**. Вы можете указать отпечатки SHA1 всей цепочки сертификатов SIEM-системы (включая корневой сертификат) в Open Single Management Platform. Чтобы добавить отпечаток SHA1, введите его в поле **Отпечатки** и нажмите на кнопку **Добавить**.

С помощью **Добавить проверку подлинности клиента** вы можете сгенерировать сертификат для аутентификации Open Single Management Platform. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Open Single Management Platform. В этом случае для аутентификации сервера SIEM-системы можно использовать как доверенный сертификат, так и отпечаток SHA.

- **Добавить имя субъекта/альтернативное имя субъекта**

  Имя субъекта – это доменное имя, для которого получен сертификат. Open Single Management Platform не может подключиться к серверу SIEM-системы, если доменное имя сервера SIEM-системы не совпадает с именем субъекта сертификата сервера SIEM-системы. Однако сервер SIEM-системы может изменить свое доменное имя, если имя изменилось в сертификате. В этом случае вы можете указать имена субъектов в поле **Добавить имя субъекта/альтернативное имя субъекта**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Open Single Management Platform проверяет сертификат сервера SIEM-системы.

- **Добавить проверку подлинности клиента**

  Для аутентификации клиента вы можете вставить свой сертификат или сгенерировать его в Open Single Management Platform.

  - **Вставить сертификат**. Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

    - **X.509-сертификат PEM**. Загрузите файл с сертификатом в поле **Файл с сертификатом** и файл с закрытым ключом в поле **Файл с ключом**. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла будут загружены, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

    - **X.509-сертификат PKCS12**. Загрузите один файл, содержащий сертификат и его закрытый ключ, в поле **Файл с сертификатом**. Когда файл будет загружен, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - **Сгенерировать ключ**. Вы можете сгенерировать самоподписанный сертификат в Open Single Management Platform. В результате Open Single Management Platform сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

- **Формат данных**

  Вы можете выбрать форматы Kaspersky SIEM (KUMA), IBM QRadar SIEM, ArcSight, Splunk или Syslog в зависимости от требований SIEM-системы.

  Если вы выбрали формат данных системного журнала, вы должны указать **Максимальный размер сообщения в байтах**

  Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Это поле доступно, только если вы выбрали формат Syslog в поле **Протокол**.

5. Заархивированные события можно экспортировать из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:

   a. Перейдите по ссылке **Установите дату начала экспорта**.

   b. В открывшемся разделе, укажите дату начала экспорта в поле **Дата начала экспорта**.

   c. Нажмите на кнопку **OK**.

6. Включите параметр **Экспортировать события в SIEM**.

7. Чтобы отправлять события изменения политик в SIEM, включите параметр **Экспорт расширенных событий для изменений политики в SIEM**. Для каждого измененного параметра политики будет отправлено отдельное событие в SIEM.

8. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить подключение**.

   Соединение с сервером SIEM-системы установлено, и отправлено тестовое событие. Отобразится статус подключения.

9. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует выбранные события или события изменения политик в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

Мониторинг изменений политики и профилей политик

При изменении параметра политики генерируется событие изменения политики, которое затем можно экспортировать в SIEM-систему для отслеживания изменений политики и создания алертов. Доступ к событиям изменения политик возможен только через SIEM-систему.

События изменения политик не сохраняются в базе данных Сервера администрирования после генерации и не могут быть просмотрены в OSMP Console в разделе **Мониторинг** → **Выборки событий**. Вы также не можете указать параметры уведомлений и параметры хранилища для этих событий на вкладке **Настройка событий**.

При создании политики событие изменения политики генерируется для каждого параметра политики. При изменении политики событие изменения политики создается для каждого измененного параметра политики. При удалении политики генерируется одно событие. Например, создание политики Kaspersky Security Center сгенерирует около 1000 событий, а создание политики Kaspersky Endpoint Security сгенерирует более 7000 событий.

Условия для генерации событий изменения политик

События изменения политик создаются, когда пользователь совершает с политикой или профилем политики любое из следующих действий:

- Создание, изменение или удаление политики.
- Создание, изменение или удаление профиля политики.
- Откат политики к выбранной ревизии.
- Импорт или копирование политики.
- Импорт или копирование профиля политики.
- Перемещение политики в другую группу администрирования.

События изменения политик генерируются при выполнении следующих условий:

- Изменены политики следующих приложений:
  - Агент администрирования Kaspersky Security Center.
  - Сервер администрирования Kaspersky Security Center.
  - Kaspersky Endpoint Security for Windows 14.1 или более поздней версии.
  - Kaspersky Endpoint Security for Linux 12.5 или более поздней версии.
  - Kaspersky Endpoint Security for Linux 12.4 или более поздней версии.
  - Kaspersky Endpoint Security for Mac 12.2.1 или более поздней версии.
- В свойствах Сервера администрирования включен параметр **Экспорт расширенных событий для изменений политики в SIEM**.
- Изменение политики осуществляется вручную через OSMP Console.

События изменения политик не создаются в следующих случаях:

- Изменены общие параметры политики.
- Изменены параметры политики, унаследованные от родительской политики.
- Параметры политики изменены через Kaspersky Security Center OpenAPI.
- Параметры приложения "Лаборатории Касперского" изменены в самом приложении.

Поля событий изменения политики

В таблице ниже показан набор полей события изменения политики. Представление этих полей зависит от формата событий (например, syslog, CEF или LEEF). Точные имена полей и шаблоны событий см. в файле siem_conversion_rules.xml. Параметры события доступны только на английском языке.

Поле события	Тип данных	Описание
`eventType`	string	Тип события. Позволяет создавать правила корреляции для определенного типа событий. Возможные значения: "Policy created", "Policy modified", "Policy deleted".
`srvName`	string	Имя Сервера администрирования.
`eventTime`	datetime	Дата и время события (в формате UTC).
`eventGroupID`	int	Идентификатор изменения группы событий.
`objectID`	int	Внутренний идентификатор объекта.
`objectName`	string	Отображаемое имя политики.
`objectGroup`	string	Полный путь и имя группы администрирования, в которой находится политика.
`user`	string	Имя пользователя, который внес изменения в политику.
`operation`	string	Тип изменения параметра. Возможные значения: "Added", "Removed", "Changed".
`path`	string	Путь к параметру. Содержит путь к родительскому узлу параметра, который был изменен. Путь создается на основе названий разделов и подразделов политики. Структура пути идентична описанной в разделах Параметры политики Агента администрирования, Общие параметры политики и Сравнение ревизий политики.
`parameter`	string	Название параметра политики, который был изменен.
`oldValue`	string	Старое значение параметра политики, который был изменен.
`newValue`	string	Новое значение параметра политики, который был изменен.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky EDR Expert, не используя интерфейс Kaspersky EDR Expert. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky EDR Expert предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky EDR Expert, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по выполнению SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky EDR Expert, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

Выполнение SQL-запроса с помощью утилиты klsql2

В этой статье приведены инструкции по использованию утилиты klsql2, а также по выполнению SQL-запроса с использованием этой утилиты. Используйте версию утилиты klsql2, которая входит в вашу установленную версию Kaspersky EDR Expert.

Чтобы использовать утилиту klsql2:

1. Перейдите в директорию, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

2. В этой директории создайте пустой файл с расширением .sql.

3. Откройте созданный файл .sql с помощью любого текстового редактора.

4. В файле .sql введите требуемый SQL-запрос и сохраните файл.

5. На устройстве, на котором установлен Сервер администрирования, в командной строке введите следующую команду для выполнения SQL-запроса из файла .sql и сохранения результатов в файл result.xml:
   ```
   sudo ./klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```
   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

6. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.

7. Откройте созданные файлы result.xml и просмотрите результаты выполнения SQL-запроса.

Вы можете изменять файл .sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, выполненного с помощью утилиты klsql2.

Следующие примеры показывают, как получить список событий, зарегистрированных на устройствах пользователей за последние 7 дней, и отсортировать их по времени возникновения. Сначала отображаются самые последние события.

Пример для PostgreSQL:

```
SELECT
  /* идентификатор события */
  "e"."nId",

  /* время возникновения события */
  "e"."tmRiseTime",

  /* внутреннее имя типа события */
  "e"."strEventType",

  /* отображаемое имя события */
  "e"."wstrEventTypeDisplayName",

  /* отображаемое описание события */
  "e"."wstrDescription",

  /* отображаемое описание события */
  "e"."wstrGroupName",

  /* отображаемое имя устройства, на котором произошло событие */
  "h"."wstrDisplayName",
  (
    CAST(("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-адрес устройства, на котором произошло событие */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Пример для MySQL или MariaDB:

```
SELECT

  /* идентификатор события */
  `e`.`nId`,

  /* время возникновения события */
  `e`.`tmRiseTime`,

  /* внутреннее имя типа события */
  `e`.`strEventType`,

  /* отображаемое имя события */
  `e`.`wstrEventTypeDisplayName`,

  /* отображаемое описание события */
  `e`.`wstrDescription`,

  /* имя группы устройств */
  `e`.`wstrGroupName`,

  /* отображаемое имя устройства, на котором произошло событие */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP-адрес устройства, на котором произошло событие */
    LEFT(CAST((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Просмотр имени базы данных Kaspersky EDR Expert

Для доступа к базе данных Kaspersky EDR Expert с помощью MySQL или MariaDB необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

Чтобы просмотреть имя базы данных Kaspersky EDR Expert:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Информация об используемой базе данных**.

   Имя базы данных указано в поле **Имя базы данных**. Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

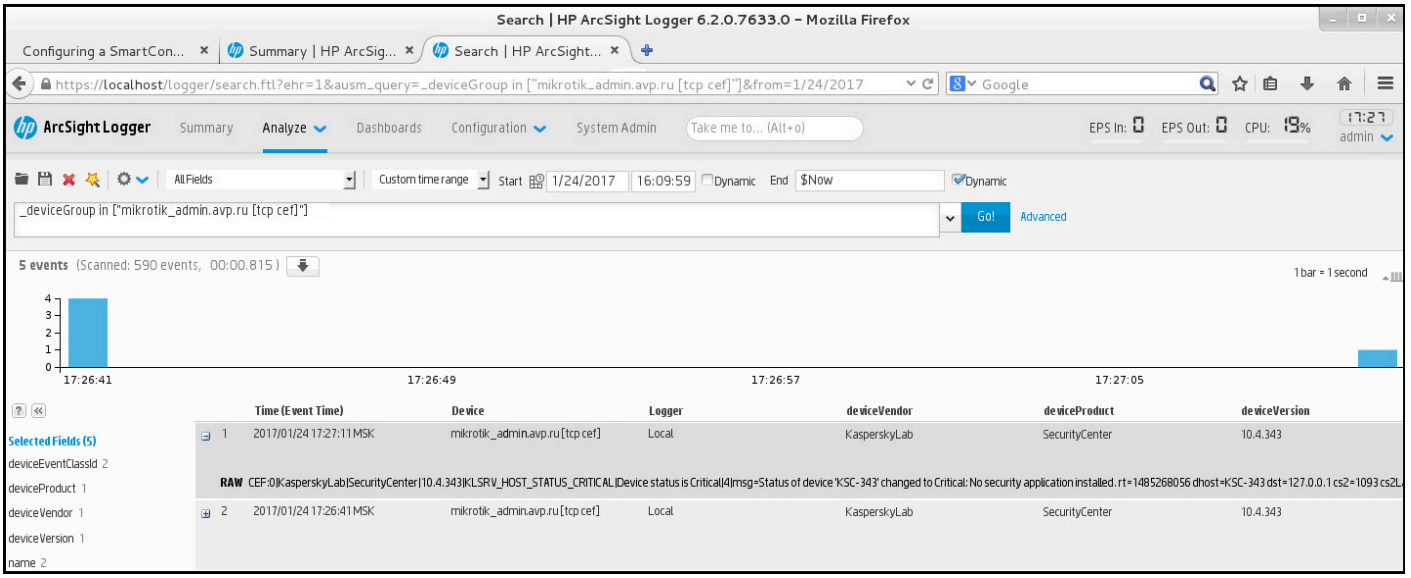
Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky EDR Expert события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky EDR Expert и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.



Пример событий

Отправка событий из коллектора OSMP в коллектор внешней SIEM-системы

Для настройки отправки событий в коллектор внешней SIEM-системы должны быть выполнены следующие условия:

1. Выполнен вход в Консоль OSMP под учетной записью пользователя с правами Главного администратора.
2. В OSMP установлен коллектор **[OOTB] Kaspersky EDR** в кластере Kubernetes.
3. В KUMA установлен коллектор со следующими компонентами:
   - Коннектор с типом **tcp** с включенным режимом TLS и разделителем \n.
   - Нормализатор с типом **json** без сопоставления и с включенным сырым событием.
   - Точка назначения с типом **storage**.
4. Доступен Unix-терминал с установленными утилитами curl и openssl.

Настройка отправки событий из коллектора OSMP в коллектор внешней SIEM-системы состоит из следующих этапов:

1. **Получение сертификата и ключа для отправки событий в коллектор [OOTB] Kaspersky EDR**

   1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
   2. Нажмите на **Тенант Root** и перейдите в подраздел **Параметры** → **Сертификаты**.
   3. Установите флажок рядом с TLS-сертификатом и нажмите на кнопку **Экспортировать**.
   4. В открывшемся окне укажите пароль и нажмите на кнопку **Экспортировать**.

      Сертификат в формате PFX будет скачан в директорию загрузок по умолчанию.
   5. Распакуйте скачанный сертификат для получения сертификата cert.pem и ключа key.pem, выполнив следующие команды:

      ```
      openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out cert.pem && \
      openssl pkcs12 -in certificate.pfx -nocerts -nodes -out key.pem
      ```

      Нужно дважды ввести пароль, указанный при экспорте сертификата PFX.

   Получены сертификат cert.pem и ключ key.pem для отправки событий в коллектор.

2. **Создание и настройка точки назначения TCP для отправки событий во внешнюю SIEM-систему**

   1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
   2. Выберите коллектор **[OOTB] Kaspersky EDR**.

3. В открывшемся окне редактирования коллектора перейдите на вкладку **Маршрутизация** и нажмите на кнопку **Добавить**.

4. Создайте точку назначения, выполнив следующие действия:

   a. На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **tcp**.

   b. В поле **URL** укажите URL, с которым необходимо установить связь. Пример: <имя_хоста_коллектора_KUMA>:<порт_коллектора_KUMA>.

   c. Перейдите на вкладку **Дополнительные параметры**.

   d. В раскрывающемся списке **Режим TLS** выберите **Включено**.

   e. В раскрывающемся списке **Разделитель** выберите **\n**.

   f. Нажмите на кнопку **Сохранить**.

5. Перейдите на вкладку **Проверка параметров** и нажмите на кнопку **Сохранить и перезапустить сервисы**.

6. Закройте окно редактирования коллектора.

Настроена точка назначения TCP с режимом TLS для отправки событий во внешнюю SIEM-систему.

3 Получение Connector gateway URL коллектора [OOTB] Kaspersky EDR

1. В разделе **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** нажмите правой кнопкой мыши на коллектор **[OOTB] Kaspersky EDR** и в контекстном меню выберите **Развернуть**.

2. В открывшемся окне скопируйте значения параметра **Connector gateway URL**.

4 Отправка тестового события в коллектор [OOTB] Kaspersky EDR

1. Выполните в терминале следующую команду:

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://<Connector gateway URL> -k
```

2. Вместо `<Connector gateway URL>` укажите значение параметра **Connector gateway URL**, скопированное ранее.

Пример

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://example.connector-gateway-url.ru:443 -k
```

В терминале отображается код ответа 200. Событие отправлено в коллектор внешней SIEM-системы.

5 **Проверка поступления события во внешнюю SIEM-систему**

1. Войдите в веб-интерфейс KUMA под учетной записью пользователя с правами Главного администратора.

2. Перейдите в раздел **События**.

3. Найдите событие со значением **Test_send_to_external_SIEM_collector** в поле **KL_HostOsFamily**.

Пример содержимого поля Raw


```
{
  "ID":"fca85cda-f760-48a8-8060-382bbaf7af14",
  "Timestamp":1776534533425,
  "TenantID":"d22648f7-bd98-4f55-a7ca-90b51f4d3fae",
  "ServiceID":"efd93e7c-1f8c-4035-bc76-a6efdd72197f",
  "ServiceName":"[OOTB] Kaspersky EDR",
  "Priority":0,
  "SpaceID":"",
  "DeviceTimeZone":"+03:00",
  "EndTime":1776534533425,
  "DeviceReceiptTime":1776534533425,
  "Type":1,
  "Extra":{
    "Product":"EDR"
  },
  "S":{
    "KL_HostOsFamily":"Test_send_to_external_SIEM_collector",
    "KL_Product":"EDR"
```


Событие поступило в коллектор внешней SIEM-системы.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky EDR Expert позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик);
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в виде файла JSON (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес Консоли OSMP, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Просмотр и сохранение ревизии политики

Ревизия политики – это сохраненное состояние политики, которое автоматически фиксируется каждый раз при ее изменении и сохранении. Ревизия сдержит параметры политики, профили и правила их активации, метаданные о дате, а также пользователе и IP-адресе, которые создали эту ревизию. Open Single Management Platform позволяет просматривать ревизию политики, чтобы отслеживать изменения настроек, а также сохранять ревизию в файл JSON.

> Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.
> Опции доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0), Kaspersky Endpoint Security for Linux (начиная с версии веб-плагина 12.4) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   В открывшемся отчете доступна информация о параметрах политики, ее профилях и правилах активации для них.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью OSMP Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

В случае политик Kaspersky Endpoint Security for Windows и Kaspersky Endpoint Security for Mac в отчете не будет информации о профилях политик.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

При необходимости вы можете сравнить ревизии политики.

Сравнение ревизий политики

Вы можете сравнить предыдущие ревизии политики с ее текущей ревизией, сравнить различные ревизии, выбранные в списке, или сравнить ревизию одной политики с ревизией другой политики. Параметры доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Сравнение ревизий политик доступно, если соответствующие веб-плагины управления поддерживает эту функцию.

Чтобы сравнить ревизии политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику, ревизии которой вы хотите сравнить.

   Откроется окно свойств политики.
3. Перейдите на вкладку **История ревизий** и установите флажки рядом с ревизиями, которые нужно сравнить.

4. В панели инструментов нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите один из следующих вариантов:

   - **С текущей ревизией**, если вы хотите сравнить ревизию, выбранную на шаге 3, с последней сохраненной ревизией той же политики.

   - **Выбранные ревизии**, если вы хотите сравнить две ревизии, около которых вы установили флажки на шаге 3.

     > Порядок установки флажков не влияет на результаты сравнения. По умолчанию более ранняя выбранная ревизия сравнивается с последней ревизией. Например, если вы установите флажки рядом с ревизиями 5 и 1, ревизия 1 будет сравниваться с ревизией 5. Отчет будет содержать информацию о параметрах ревизии 1, которые были добавлены, удалены или изменены по сравнению с ревизией 5.

   - **С ревизией другой политики**, если вы хотите сравнить ревизии двух разных политик.

     В открывшейся правой панели выполните следующее:

     a. В поле **Название приложения** выберите политику, ревизии которой вы хотите сравнить: Агент администрирования или Сервер администрирования.

     b. В поле **Название политики** укажите название политики, ревизию которой вы хотите сравнить с той, которую вы выбрали на шаге 3.

     Отобразится список ревизий политики.

     c. Выберите нужную ревизию и нажмите на кнопку **Сравнить**.

Отчет сравнения ревизий отобразится в формате HTML на новой вкладке вашего браузера.

> Если результат сравнения превышает 10 МБ, отобразится соответствующее диалоговое окно. Вы можете нажать на кнопку **Сохранить в файл**, чтобы сохранить отчет в виде файла, или отменить операцию.

Отчет отображается на языке интерфейса вашего приложения OSMP Console. Вы можете развернуть некоторые разделы отчета, нажав на значок стрелки вниз (▼) рядом с разделом или свернуть раздел, нажав на значок стрелки вверх (▲).

Отчет содержит следующую информацию:

- Логотип "Лаборатория Касперского".
- Название отчета.
- Время и дата создания отчета.
- Имя политики, Сервер администрирования и группа администрирования, в которую входит политика (политики), ревизии которой сравнивались.
- Кнопка **Сохранить как HTML**. Если вы нажмете на кнопку, отчет будет сохранен на вашем устройстве.

- Раздел **Сводная информация**, в котором отображается общая информация о сравниваемых ревизиях: имя политики (политик), номер ревизии, время и дата, когда ревизия была сохранена, пользователь, который сохранил ревизию, и описание ревизии.

  Для унаследованных политик пользователь не отображается.

- Различия сравниваемых ревизий. Различия отображаются в следующих разделах:

  - **Добавленные параметры.**
  - **Удаленные параметры.**
  - **Измененные параметры.**
  - **Параметры доступны только для объекта 1** (если вы сравнивали ревизии двух разных политик).
  - **Параметры доступны только для объекта 2** (если вы сравнивали ревизии двух разных политик).

  Раздел не отображается, если в нем нет данных.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

   Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Операции по диагностике компонентов Kaspersky EDR Expert

В этом разделе описано, как получить диагностическую информацию о компонентах Kaspersky EDR Expert.

Получение файлов журнала компонентов Kaspersky EDR Expert

KDT позволяет получать файлы журнала, которые содержат диагностическую информацию о компонентах Kaspersky EDR Expert и кластере Kubernetes, что позволяет устранять проблемы самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Kaspersky EDR Expert генерирует имена файлов журнала по следующему шаблону: pod_name.container_name.log. Здесь pod_name – это имя пода Kubernetes, container_name – это имя контейнера Kubernetes.

Чтобы получить файлы журнала компонентов Kaspersky EDR Expert и веб-плагинов управления,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt logs get <flags>
```

Где `<flags>` – параметры команды, которая позволяет настроить результат сохранения событий.

Вы можете указать следующие параметры ведения журнала событий:

- `--app < список_компонентов >` – получить журналы событий для перечисленных компонентов Kaspersky EDR Expert.

  Например, если требуется получить журнал Сервера администрирования за последний час, выполните следующую команду:

  ```
  ./kdt logs get --app ksc
  ```

  Список доступных компонентов Kaspersky EDR Expert

  ```
  account

  action-registry

  agent-server-responser

  agentserver

  aggregator

  asset-account

  asset-manager

  backup-operator

  collector

  comment

  component
  ```

configuration

core

correlator

credentials

db-operator

decision-point

detects-processor

enricher

file-registry

gateway

gateway-operator

grafana

graph

hierman

iamoperator

istio-cni

istiod

kata-proxy

ksb-facade

ksc

ksc-info

ksc-tenant-binder

kscadapter

kubernetes-event-exporter

kube-state-metrics

kuma-operator

kuma-proxy

licensing-policy

local-path-provisioner

longhorn

loki

metallb

metrics

nats

ncircc

openbao

openbao-agent-injector

openbao-csi-provider

openbao-legacy-vault-csi-provider

operator

orchestra

osmp-scanner-facade

playbook-matcher

playbook-statistics

plugin-admin-agent

plugin-admin-server

plugin-agent-server

plugin-asset-management

plugin-enterprise

plugin-irp

plugin-kata

plugin-kes-linux

plugin-kesw

plugin-kuma

plugin-osmp-scanner

plugin-public-api-token-settings

plugin-spp

plugin-tenant-manager

plugin-tenant-roles

prevention-rules

prometheus-node-exporter

prometheus-redis-exporter

promtail

proxy

public-api

redis

reputation

response-manager

responser

rights

sandbox-scan-api

scan-rules-manager

scheduler

seaweedfs

secrets-store-csi-driver

ssh-remote-executor

storage

tenant-registry

tokenhub

tracker

transformer

```
unsealer

updater

updater-facade

victoria-metrics-operator

vmagent

vmalert

vmsingle

vtproxy

ztunnel
```

- `--auto-dest-dir` – получить журналы событий и сохранить их в директории kdt-default-logs-<current_date_and_time>, которая автоматически создается в текущей директории. Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.

  Например, если вы хотите получить журналы событий за последний час для Сервера администрирования и KUMA и сохранить эти журналы событий в автоматически созданной директории, выполните команду:

  ```
  ./kdt logs get --app ksc,core --auto-dest-dir
  ```

- `-d, --destination <путь_к_файлу>` – получить журналы событий и сохранить их в указанном файле.

- `-D, --destination-dir <путь_к_директории>` – получить журналы событий и сохранить их в указанной директории, которая должна быть создана заранее. Если параметр `<directory_path>` пуст, журналы событий сохраняются в стандартном потоке вывода (stdout). Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.

- `--to-archive` – получить журналы событий и сохранить их в kdt-default-logs-<current_date_and_time>.tar.gz. Созданный архив сохраняется в текущей директории. Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.

- `--last=<часы>h` – получить журналы событий за указанное количество часов в актуальном состоянии.

  Например, если вы хотите получить архив с журналами за последние три часа, выполните команду:

  ```
  ./kdt logs get --to-archive --last=3h
  ```

- `--start=<дата_и_время>` – получить журналы событий, начиная с указанной даты и времени (в формате Unix timestamp) до настоящего времени или до даты и времени, указанных в параметре `--end`.

  Например, если вы хотите получить журналы с 26.03.2024 10:00:00 по настоящее время и сохранить их в директории kdt-default-logs-<current_date_and_time>, созданной в текущей директории, выполните команду:

  ```
  ./kdt logs get --auto-dest-dir --start=1711447200
  ```

- `--end=<дата_и_время>` – получить журналы событий, начиная с даты и времени, указанных в параметре `--start`, до даты и времени, указанных в параметре `--end` (в формате Unix timestamp). Если параметр `--start` не указан, журналы событий будут получены за последний час до даты и времени, заданных параметром `--end`.

  Например, если вы хотите сохранить журналы событий за 10 минут (с 26.03.2024 10:00:00 до 26.03.2024 10:10:00) в директории журналов событий, выполните команду:

```
./kdt logs get -D ./logs/ start=1711447200 --end=1711447800
```

Для того чтобы просмотреть доступные параметры ведения журнала, вы можете выполнить одну из следующих команд:

- `./kdt logs get -h`
- `./kdt logs get --help`

Просмотр метрик OSMP

Компонент наблюдаемости Kaspersky EDR Expert позволяет просматривать метрики OSMP, отслеживать статус каждого компонента с помощью панели мониторинга, просматривать показатели системы хранения данных (Longhorn) для кластера Kubernetes и уведомлять пользователей по электронной почте, если показатели производительности узла кластера Kubernetes превышают нормальные значения.

Вы можете отслеживать показатели для дальнейшего анализа работоспособности и производительности компонентов с помощью компонента наблюдаемости.

Вы можете просмотреть метрики OSMP одним из следующих способов:

- С помощью панелей мониторинга Grafana.
- С помощью собственных инструментов мониторинга.

Чтобы просмотреть метрики OSMP с помощью панелей мониторинга Grafana:

1. Перейдите по веб-адресу `<monitoring_host>.<smp_domain>`.

   Где `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры представляют собой FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert.

2. Введите учетные данные Grafana, указанные в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

Также метрики OSMP можно просмотреть в разделе **Панель мониторинга**:

1. В главном меню перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Нажмите на значок с многоточием (⋮).
3. Нажмите на кнопку Перейти к метрикам OSMP.

   Отображается интерфейс Grafana. Вы можете просматривать диагностическую информацию для каждого компонента Kaspersky EDR Expert и показатели системы хранения данных (Longhorn) для кластера Kubernetes, а также настраивать уведомления по электронной почте о событиях работоспособности кластера Kubernetes.

Чтобы просмотреть метрики OSMP с помощью собственных инструментов мониторинга:

1. Настройте инструменты мониторинга для получения метрик из API Kaspersky EDR Expert.

2. Перейдите по адресу API `<api_host>.<smp_domain>/api/read-api`, чтобы получить метрики.

   Где `<api_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры составляют FQDN сервиса, обеспечивающего доступ к API Kaspersky EDR Expert. Эти параметры задаются в конфигурационном файле при развертывании Kaspersky EDR Expert.

Метрики OSMP в формате OpenMetrics получены.

Если вы хотите просмотреть информацию о производительности Ядра KUMA, хранилища, коллекторов и корреляторов, вам необходимо просмотреть метрики KUMA.

Мониторинг состояний компонентов Kaspersky EDR Expert

Панель мониторинга предоставляет собой графическое отображение состояния каждого компонента Kaspersky EDR Expert.

Например, вы можете просмотреть следующие параметры компонента:

- использование запросов и ограничений процессора;
- использование запросов процессора и оперативной памяти;
- использование процессора и оперативной памяти контейнерами;
- распределение ресурсов компонентов контейнерами;
- Индикаторы производительности сети:
  - Сглаживание
  - Полученные пакеты (количество полученных пакетов)
  - Потерянные пакеты (количество потерянных пакетов)
  - Ошибки (количество сетевых ошибок)

Чтобы просмотреть диагностическую информацию в панели мониторинга:

1. Перейдите по веб-адресу `<monitoring_host>.<smp_domain>`.

   Где `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры представляют собой FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert. Например: `monitoring.smp.local`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В меню перейдите в раздел **Главная** → **Панели мониторинга** → **Kubernetes / Просмотры / Поды**.

4. В раскрывающемся списке **namespace** выберите компонент, для которого вы хотите просмотреть диагностическую информацию.

5. Вы также можете указать другие параметры для настройки вида панели мониторинга.

   Отображается панель мониторинга с диагностической информацией о выбранном компоненте Kaspersky EDR Expert.

Просмотр метрик Longhorn

Kaspersky EDR Expert включает панель мониторинга, на которой отображаются ключевые метрики системы хранения данных кластера (Longhorn). Панель мониторинга Longhorn позволяет отслеживать состояние и производительность хранилища данных.

По умолчанию в панели мониторинга отображаются данные за последние три часа. Этот период можно изменить. Панель мониторинга обновляется каждые 15 секунд.

Чтобы просмотреть панель мониторинга Longhorn:

1. Перейдите на `<monitoring_host>.<smp_domain>`.

   `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Вместе эти параметры формируют FQDN службы мониторинга Kaspersky EDR Expert и задаются в конфигурационном файле при развертывании Kaspersky EDR Expert.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (`grafana_admin_user` и `grafana_admin_password`).

3. В меню перейдите в раздел **Home** → **Dashboards** → **Longhorn Dashboard**.

   Отобразится панель мониторинга Longhorn.

Метрики панели мониторинга Longhorn описаны ниже.

Узлы

- **Nodes** – общее количество узлов в системе.
- **Schedulable Nodes** – количество узлов, доступных для распространения реплик тома.
- **Disabled Nodes** – узлы, которые пользователь выключил.
- **Failed Nodes** – узлы, которые не отвечают, выключенные или недоступные по иным причинам.

Тома

- **Attached Volumes** – тома, которые в текущий момент прикреплены к узлам.
- **Detached Volumes** – тома, которые не прикреплены к узлам.
- **Degraded Volumes** – тома с недостаточным количеством реплик.
- **Faulty Volumes** – тома, работающие без функциональности реплик.

Объем

- **Node Capacity** – общий объем хранилища на каждом узле.
- **Disk Capacity** – объем дискового пространства каждого диска.
- **Volume Capacity** – объем каждого тома.

Использование ресурсов

- **Node Storage Usage/Capacity** – процент объема хранилища на каждом узле.
- **Disk Space Usage** – процент объема на каждом диске.
- **Volumes Per Node** – количество подключенных томов на каждом узле.
- **Volume Size/Capacity** – отношение реального размера томов к их максимальному объему.
- **Volume Write Throughput** – объем данных, которые система записывает в секунду (бит/с).
- **Volume Read Throughput** – объем данных, которые система читает в секунду (бит/с).
- **Volume Write IOPS** – количество операций записи ввода/вывода (IOPS).
- **Volume Read IOPS** – количество операций чтения ввода/вывода (IOPS).
- **Volume Write Latency** – время, необходимое для выполнения одной операции записи (нс).
- **Volume Read Latency** – время, необходимое для выполнения одной операции чтения (нс).
- **Node CPU Usage/Capacity** – процент использования процессора на узле.
- **Node Memory Usage/Capacity** – процент использования памяти на узле.
- **Longhorn Manager CPU Usage** – загрузка процессора Longhorn Manager Longhorn (в миллипроцессорных единицах).
- **Longhorn Manager Memory Usage** – загрузка памяти Longhorn Manager Longhorn.
- **Instance Manager CPU Usage** – загрузка процессоров экземпляров Longhorn (в миллипроцессорных единицах).
- **Instance Manager Memory Usage** – память, используемая экземплярами Longhorn.

Использование диска

Индикаторы в панели использования диска отображают процент времени, которое диск тратит на чтение и запись. Эти индикаторы основаны на следующих метриках:

- `longhorn_volume_read_iops`
- `longhorn_volume_read_latency_seconds`

- `longhorn_volume_write_iops`
- `longhorn_volume_write_latency_seconds`

Просмотр панелей мониторинга и метрик EDR

Kaspersky EDR Expert представляет панели мониторинга EDR, на которых отображаются метрики компонентов решения, отвечающие за обработку объектов от Endpoint Agent. Мониторинг этих метрик помогает обеспечить бесперебойную и безопасную работу компонентов, позволяя заранее принимать меры по предотвращению возможных проблем.

Доступны следующие панели мониторинга:

- EDR Agent Server
- EDR KSB
- EDR KSN proxy
- EDR Sandbox
- EDR Scanner

Чтобы просмотреть панели мониторинга EDR:

1. Перейдите на `<monitoring_host>.<smp_domain>`.

   `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Вместе эти параметры формируют FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (`grafana_admin_user` и `grafana_admin_password`).

3. В меню перейдите в раздел **Главная** → **Панели мониторинга**.

4. В раскрывающемся меню фильтрации по тегам (**Фильтрация по тегам**) выберите тег **edr**.

   Отобразится список доступных панелей мониторинга EDR.

5. Нажмите на имя панели мониторинга, которую хотите просмотреть.

   Откроется выбранная панель мониторинга.

Ниже описаны виджеты и метрики, которые доступны на каждой панели мониторинга EDR.

EDR Agent Server

По умолчанию в панели мониторинга отображаются данные за последние два дня. Вы можете изменить этот период, нажав **Последние 2 дня** в верхней части страницы и указав нужный период.

Имя виджета	Название метрики	Описание
Задачи.	xdr_agentserver_tasks_total	Общее количество задач, полученных от Incident Response Platform.
Settings	xdr_agentserver_settings_total	Общее количество конфигураций, полученных от Incident Response Platform.
Выполняемые задачи	xdr_agentserver_tasks_active	Общее количество задач в обработке.
Действующие настройки	xdr_agentserver_settings_active	Общее количество приложений конфигурации в обработке.
Ошибки задач	xdr_agentserver_tasks_errors_total	Общее количество задач, завершившихся с ошибкой.
Ошибки настроек	xdr_agentserver_settings_errors_total	Общее количество ошибок приложений конфигурации.
Object Storage	xdr_agentserver_objectstorage_upload_errors_total	Общее количество ошибок загрузки файлов в Object Storage.
Object Storage	xdr_agentserver_objectstorage_download_errors_total	Общее количество ошибок при загрузке файлов из Object Storage.
Обновление информации Agent	xdr_agentserver_agentinfo_updates_total	Общее количество раз, обновления информации о Endpoint Agent и отправки этой информации в разделе Управление активами.
Ошибки решения активов	xdr_agentserver_assets_resolve_errors_total	Общее количество ошибок сопоставления идентификаторов между OSMP и Endpoint Agent.
Активы	xdr_agentserver_assets_resolve_total	Общее количество решений.
Превышена частота срабатываний Agent	xdr_agentserver_rate_limit_exceeded_total	Общее количество случаев превышения предельного количества срабатываний.
Аутентификация Agent	xdr_agentserver_agent_auth_total	Общее количество попыток аутентификации Endpoint Agent.
Аутентификация Agent	xdr_agentserver_agent_auth_errors_total	Общее количество ошибок аутентификации Endpoint Agent.
Сеансы Vtproxy	xdr_agentserver_vtproxy_sessions_total	Общее количество созданных сеансов.
Ошибки аутентификации Vtproxy	xdr_agentserver_vtproxy_auth_errors_total	Общее количество ошибок аутентификации сеанса.
Успешные аутентификации Vtproxy	xdr_agentserver_vtproxy_successful_auths_total	Общее количество успешных аутентификаций сеанса.
Активные сеансы сенсора Vtproxy	xdr_agentserver_vtproxy_sensor_session_active	Активные сеансы сенсора.
Активные сеансы Vtproxy	xdr_agentserver_vtproxy_sessions_active	Количество активных сеансов.
Длительность сеансов Vtproxy	xdr_agentserver_vtproxy_session_duration_seconds	Длительность сеансов (в секундах).
Переданные байты Vtproxy	xdr_agentserver_vtproxy_bytes_transferred_total	Общее количество переданных байтов.

EDR KSB

По умолчанию в панели мониторинга отображаются данные за последние два дня. Вы можете изменить этот период, нажав **Последние 2 дня** в верхней части страницы и указав нужный период.

Виджеты и метрики EDR KSB

Название виджета	Название метрики	Описание
Множественные задачи	xdr_ksb_multitasks_total	Общее количество задач проверки.
Выполняемые множественные задачи	xdr_ksb_multitasks_active	Количество выполняемых задач проверки.
Дубликаты множественных задач	xdr_ksb_multitask_duplicates_total	Количество дубликатов задач проверки.
Дубликаты файлов множественных задач	xdr_ksb_multitask_file_duplicates_total	Количество дубликатов файлов в задачах проверки.
Размер файлов множественных задач	xdr_ksb_multitask_files_size_bytes_total	Размер файлов множественных задач (в байтах).
Ошибки аутентификации Agent	xdr_ksb_agent_auth_failures_total	Количество ошибок аутентификации Endpoint Agent.
Превышение лимита частоты срабатываний	xdr_ksb_rate_limit_exceeded_total	Общее количество случаев превышения предельного количества срабатываний.

EDR KSN proxy

По умолчанию в панели мониторинга отображаются данные за последние шесть часов. Вы можете изменить этот период, нажав **Последние 6 часов** в верхней части страницы и указав нужный период.

Виджеты и метрики прокси-сервера EDR KSN

Название виджета	Название метрики	Описание
Сообщения по статистике	xdr_scanner_ksnproxyfacade_stats_messages_total	Общее количество сообщений по статистике.
Изменения режима интеграции	xdr_scanner_ksnproxyfacade_integration_mode_changes_total	Общее количество изменений типа интеграции.
Запуски прокси-сервера KSN	xdr_scanner_ksnproxysupervisor_ksnproxy_starts_total	Общее количество запусков прокси-сервера KSN.
Ошибки запуска прокси-сервера KSN	xdr_scanner_ksnproxysupervisor_ksnproxy_start_errors_total	Общее количество ошибок запуска прокси-сервера KSN.
Доступность KSN	xdr_scanner_ksnproxy_ksn_proxy_ksn_available	Доступность KSN.
Ошибки при запросах периодического сигнала KSN	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_failed_requests_total	Общее количество ошибок при запросах периодического сигнала.
Запросы периодического сигнала KSN	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_requests_total	Общее количество запросов периодического сигнала.

EDR Sandbox

По умолчанию в панели мониторинга отображаются данные за последние шесть часов. Вы можете изменить этот период, нажав **Последние 6 часов** в верхней части страницы и указав нужный период.

Чтобы просмотреть показатели конкретной Sandbox, выберите ее IP-адрес в меню **Sandbox** в верхней части экрана.

Виджеты и метрики EDR Sandbox

Название виджета	Название метрики	Описание
Start time Uptime	xdr_scanner_sb_process_start_time_seconds	Время запуска процесса Sandbox и время его работы (в секундах).
Последняя проверка работоспособности Sandbox Ошибки проверки работоспособности SB	xdr_scanner_sb_health_check_errors_current	Время последней проверки работоспособности и текущее число обнаруженных ошибок.
Время с последнего обновления баз SB	xdr_scanner_sb_health_bases_age_seconds	Время с последнего обновления антивирусных баз Sandbox (в секундах).
Процессор	xdr_scanner_sb_process_cpu_seconds_total	Количество используемых ядер CPU.
Использование памяти	xdr_scanner_sb_go_memstats_sys_bytes	Память, запрошенная у системы (в байтах).
Memory usage	xdr_scanner_sb_go_memstats_heap_inuse_bytes	Объем используемой памяти heap (в байтах).
Memory usage	xdr_scanner_sb_go_memstats_stack_inuse_bytes	Объем используемой памяти stack (в байтах).
Memory usage	xdr_scanner_sb_process_resident_memory_bytes	Резидентная память (RSS) в байтах.
Запись/чтение с диска	xdr_scanner_sb_node_disk_read_bytes_total	Общее количество байтов, прочтенных с диска.
Disk writes/reads	xdr_scanner_sb_node_disk_written_bytes_total	Общее количество байтов, записанных на диск.
Использование сети	xdr_scanner_sb_process_network_receive_bytes_total	Входящий трафик.
Network usage	xdr_scanner_sb_process_network_transmit_bytes_total	Исходящий трафик.
Доступность канала для вредоносного ПО	xdr_scanner_sbscanapi_sb_malware_channel_availability	Доступность канала для вредоносного ПО для конкретной Sandbox.
Статус образов SB	xdr_scanner_sb_vm_images_status	Текущий статус виртуальных машин в Sandbox, показывающий, установлены ли операционные системы.
Статус версии образа SB	xdr_scanner_sb_vm_image_version_status	Статус версий образов, используемых на виртуальных машинах, указывающий, является ли каждая версия корректной.

EDR Scanner

По умолчанию в панели мониторинга отображаются данные за последние два дня. Вы можете изменить этот период, нажав **Последние 2 дня** в верхней части страницы и указав нужный период.

В меню **Модуль проверки** в верхней части экрана выберите модуль проверки, чтобы просмотреть его метрики:

- **AM**: метрики Anti-Malware Engine
- **YARA**: метрики YARA
- **SB**: метрики Sandbox

Виджеты и метрики EDR Scanner

Название виджета	Название метрики	Описание
Последнее обновление баз	xdr_scanner_updater_updater_bases_age	Время, прошедшее с момента последнего обновления баз источника обновлений.
Last bases update	xdr_scanner_updater_updater_retranslation_age	Время, прошедшее с момента последней трансляции баз источника обновлений.

Название виджета	Название метрики	Описание
Last bases update	xdr_scanner_internalscanner_am_bases_age	Время, прошедшее с момента последнего обновления антивирусных баз Anti-Malware Engine.
Last bases update	xdr_scanner_sb_health_bases_age_seconds	Время, прошедшее с момента последнего обновления антивирусных баз в Sandbox (в секундах).
Завершенные проверки модуля AM Завершенные проверки модуля SB Завершенные проверки модуля YARA	xdr_scanner_internalscanner_scan_engine_complete_total	Количество выполненных задач проверки для каждого модуля проверки и результат проверки объекта.
Состояние проверки	xdr_scanner_internalscanner_total_scans	Количество проверок.
Scan health	xdr_scanner_internalscanner_failed_scans	Количество неудачных проверок.
Задачи проверки AM	xdr_scanner_internalscanner_am_queue_len	Количество задач, которые стоят в очереди на выполнение Anti-Malware Engine.
AM scan tasks	xdr_scanner_internalscanner_am_queue_total_items	Общее количество задач во всех очередях Anti-Malware Engine.
AM scan tasks	xdr_scanner_internalscanner_am_queue_failed_items_total	Общее количество задач, завершенных с ошибкой, в очередях Anti-Malware Engine.
Размер очереди AM	xdr_scanner_internalscanner_am_queue_size	Размер файловой системы, которая используется для очереди Anti-Malware Engine.
AM queue size	xdr_scanner_internalscanner_am_storage_size_limit	Максимально допустимый размер очереди Anti-Malware Engine.
Задачи проверки SB	xdr_scanner_internalscanner_sb_wait_queue_len	Количество задач в очереди Sandbox в OSMP Scanner.
SB scan tasks	xdr_scanner_internalscanner_sb_queue_total_items	Общее количество задач во всех очередях Sandbox.
SB scan tasks	xdr_scanner_internalscanner_sb_queue_failed_items_total	Общее количество задач, завершенных с ошибкой, в очередях Sandbox.
SB scan tasks	xdr_scanner_internalscanner_sb_queue_len	Количеством задач в очереди Sandbox.
Размер очереди SB	xdr_scanner_internalscanner_sb_queue_size	Приблизительный размер данных (выборок) в очереди Sandbox.
SB queue size	xdr_scanner_internalscanner_sb_storage_size_limit	Максимально допустимый размер очереди Sandbox.
Среднее время проверки Sandbox	xdr_scanner_sbscanapi_sb_scan_time_total	Общее время проверки Sandbox.
Average sandbox scan time	xdr_scanner_sbscanapi_sb_scan_count_total	Общее количество проверок в Sandbox.
Задачи проверки YARA	xdr_scanner_internalscanner_yr_queue_len	Количество задач в очереди YARA.
Размер очереди YARA	xdr_scanner_internalscanner_yr_queue_size	Размер файловой системы, используемой очередью YARA.
Размер очереди YARA	xdr_scanner_internalscanner_yr_storage_size_limit	Максимальный размер очереди YARA.
YARA scan tasks	xdr_scanner_internalscanner_yr_queue_total_items	Общее количество задач во всех очередях YARA.
YARA scan tasks	xdr_scanner_internalscanner_yr_queue_failed_items_total	Общее количество задач, завершенных с ошибкой, в очередях YARA.
Last bases update	xdr_scanner_internalscanner_am_bases_age	Время, прошедшее с момента последнего обновления антивирусных баз Anti-Malware Engine.

Просмотр панели мониторинга Node Exporter Full

В панели мониторинга Node Exporter Full отображены ключевые метрики производительности для узлов кластера.

Чтобы просмотреть панель инструментов Node Exporter Full:

1. Перейдите на `<monitoring_host>.<smp_domain>`.

   `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Вместе эти параметры формируют FQDN службы мониторинга Kaspersky EDR Expert и указываются в конфигурационном файле при развертывании Kaspersky EDR Expert.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (`grafana_admin_user` и `grafana_admin_password`).

3. В меню перейдите в раздел **Home** → **Dashboards**.

4. Нажмите **Node Exporter Full**.

   Откроется панель мониторинга.

По умолчанию на панели мониторинга отображаются данные за последние 24 часа. Вы можете изменить этот период, нажав **Последние 24 часов** в верхней части страницы и указав требуемый период.

Панели, доступные на панели мониторинга, описаны в таблице ниже.

Панели Node Exporter Full

Панель	Описание
Краткий обзор процессора/памяти/диска	Краткий обзор основных ресурсов: загрузка процессора и использование памяти и диска.
Pressure	Pressure Stall Information (PSI): процессор, память и ввод-вывод. Показывает точки нагрузки в системе.
Занятость процессора	Время, в течение которого процессоры заняты вычислениями (пользовательское + системное время, в процентах).
Нагрузка системы	Средняя нагрузка системы (средняя нагрузка) за 1, 5 и 15 минут.
Использование RAM	Используемая RAM, включая буферы и кеш.
Использование SWAP	Используемое пространство подкачки.
Использование корневой файловой системы	Место, используемое в корневой файловой системе (/).
Ядра процессора	Количество ядер (vCPU) на узле.
Время работы	Время, прошедшее с момента последней загрузки системы.
Общий размер RootFS	Общий размер корневой файловой системы.
Общий объем RAM	Общий объем RAM.
Общий объем SWAP	Общий объем доступной памяти подкачки.
Базовые данные процессора/памяти/сети/диска	Обзор основных метрик процессора, памяти, сети и диска.
Базовые данные процессора	Панель с базовой нагрузкой процессора, включая метрики user/system/idle/iowait.
Memory Basic	Метрики использования оперативной памяти и подкачки.
Базовые данные сетевого трафика	Общий сетевой трафик (входящий/исходящий) по интерфейсам.
Базовое используемое место на диске	Использование места на диске и разбиение на разделы.

Панель	Описание
Процессор	Подробные показатели использования процессора (по ядрам, в процентах).
Схема памяти	Использование слоев памяти (используемая, кеш, буферы, свободная).
Сетевой трафик	Общий сетевой трафик (байты/сек) по интерфейсам.
Используемое место на диске	Подробное описание используемого места на диске по разделам.
Дисковые операции ввода-вывода	Количество операций ввода-вывода в секунду (операции ввода-вывода/сек).
Чтение/запись при использовании ввода-вывода	Скорость чтения и записи данных на диски (байт/с).
Использование ввода-вывода	Использование запоминающего устройства: время, в течение которого диск выполняет операции ввода-вывода (в процентах).
Время, потраченное процессором на гостей (ВМ)	Время работы процессора, потраченное на гостевые виртуальные машины (время в гостевой системе).
Активная/неактивная память	Активные и неактивные страницы памяти (используемые и те, которые можно восстановить).
Выделенная память	Объем памяти, выделенной процессам (включая избыточную).
Подробности об активной/неактивной памяти	Подробности об активных и неактивных страницах, включая anon/file.
Обратная запись и память dirty	Количество страниц, ожидающих записи на диск (dirty, обратная запись).
Совместная и отображаемая память	Совместная и отображаемая память.
Память slab	Память, выделенная объектам ядра (slab, освобождаемая/неосвобождаемая).
Память Vmalloc	Выделение виртуальной памяти ядра.
Отказы памяти	Количество отказов страниц (редко, для старого оборудования).
Анонимная память	Анонимная память (не поддерживается файлами).
Память ядра/процессора	Память, используемая ядром и структурами процессора.
Счетчик памяти HugePages	Количество используемых больших страниц (HugePages).
Размер памяти HugePages	Размер и состояние HugePages.
Память DirectMap	Прямое отображение физической памяти (DirectMap).
Неустранимая и заблокированная память	Память, заблокированная в RAM (неустранимая и заблокированная).
Память NFS	Использование памяти подсистемой NFS.
Память Meminfo	Общая информация из /proc/meminfo.
Входящие/исходящие страницы памяти	Количество страниц, загруженных в память и выгруженных из нее.
Подкачка страниц памяти	Страницы, перемещенные между RAM и подкачкой.
Ошибки страниц памяти	Количество ошибок, связанных со страницами (незначительных и серьезных).
Завершение процессов (OOM)	События, при которых система завершала процессы из-за нехватки памяти.
Память Vmstat	Расширенная статистика виртуальной памяти (/proc/vmstat).
Расхождение в синхронизации времени	Разница между системным временем и источником синхронизации.
Настройка времени (PLL)	Параметры настройки времени (PLL, смещение).
Состояние синхронизации времени	Состояние синхронизации времени (например, chrony/ntpd).
Другие показатели времени	Другие показатели, связанные со временем (смещение, фазовое дрожание).
Синхронизация времени в системе	Общее состояние синхронизации времени на узле.
Статус процессов	Статистика процессов по состоянию (запущен, спит, зомби).
Состояние процессов	Диаграмма состояний процессов.
Порожденные процессы	Количество созданных процессов (forks).
Память процессов	Использование памяти процессами.
Количество и лимит PID	Текущее и максимальное количество PID в системе.

Панель	Описание
Статистика распределения процессов ("запущен"/"ожидает")	Распределение процессов по статусам "Запущено" и "Ожидает".
Количество и лимит потоков	Количество потоков и системный лимит.
Переключение контекста/прерывания	Переключения контекста и аппаратные прерывания.
Системная нагрузка	Средняя нагрузка за 1, 5 и 15 минут.
Масштабирование частоты процессора	Текущая частота процессора и ее масштабирование (регулятор, минимум/максимум).
Pressure Stall Information	Нагрузка процессора, памяти и ввода-вывода – показывает задержки при выполнении задач.
Подробности о прерываниях	Подробная информация по типам прерываний.
Временные интервалы каждого процессора	Количество квантов времени, выполненных каждым ядром.
Энтропия	Доступная энтропия (качество генерации случайных чисел).
Время работы процессора (пользователи/система)	Общее время процессора, проведенное в пользовательском и системном режимах.
Дескрипторы файлов	Количество открытых файловых дескрипторов.
Отслеживание аппаратной температуры	Температура компонентов системы (процессор, диски, датчики).
Устройство охлаждения	Состояние систем охлаждения и защиты от перегрева.
Электропитание	Данные о питании (напряжение, ток, блок питания).
Сокеты systemd	Активные сокеты systemd.
Состояние юнитов systemd	Состояние юнитов systemd (активен, ошибка, неактивен).
Завершенные операции ввода-вывода на диске	Завершенные операции ввода-вывода.
Чтение/запись данных на диск	Объем прочтенных/записанных данных.
Среднее время ожидания диска	Среднее время ожидания операций ввода-вывода.
Средний размер очереди	Средняя длина очереди операций ввода-вывода.
Объединение чтения/записи данных	Количество объединенных операций чтения и записи.
Время ввода-вывода	Время, затраченное на операции ввода-вывода.
Мгновенный размер очереди	Текущая длина очереди операций ввода-вывода.
Завершенные/объединенные отмены операций ввода-вывода на диске	Завершенные/объединенные отмены операций (TRIM).
Доступное место в файловой системе	Доступное место в файловых системах.
Свободные узлы файлов	Количество свободных индексных дескрипторов.
Дескриптор файла	Количество файловых дескрипторов.
Размер файловых узлов	Размер таблицы индексных дескрипторов.
Файловая система ("Только чтение"/"Ошибка")	Состояние файловой системы (ошибки, монтирование только для чтения).
Сетевой трафик по пакетам	Количество пакетов Rx/Tx по каждому интерфейсу.
Ошибки сетевого трафика	Ошибки передачи и приема трафика.
Потеря пакетов сетевого трафика	Потерянные пакеты.
Сжатый сетевой трафик	Сжатый трафик.
Многоадресная рассылка сетевого трафика	Многоадресный трафик.
Сетевой трафик FIFO	Ошибки FIFO в интерфейсах.
Фрейм сетевого трафика	Ошибки, связанные с фреймами.
Оператор сетевого трафика	Ошибки на уровне ссылок (оператор трафика).
Коллизии сетевого трафика	Сетевые коллизии.
Conntrack NF	Количество отслеживаемых сетевых подключений (conntrack).

Панель	Описание
Записи ARP	Таблица ARP (количество записей).
MTU	Максимальный размер пакета (MTU).
Скорость	Скорость сетевого интерфейса (биты/сек).
Длина очереди	Длина очереди пакетов интерфейса.
Пакеты Softnet	Обработка пакетов Softnet (ядро).
Нехватка квоты Softnet	Количество пакетов, потерянных из-за переполнения Softnet.
Состояние работы сети	Текущее состояние интерфейса (работает/не работает).
Sockstat TCP/UDP/FRAG/RAW	Статистика для TCP, UDP и сокетов других протоколов.
Размер памяти/используемая память сокетов	Использование памяти сокетами и количество активных сокетов.
Входящие/исходящие IP-октеты Netstat	Количество входящих/исходящих IP-пакетов (в байтах).
Перенаправление IP Netstat	Статус переадресации IP.
Входящие/исходящие ICMP-пакеты и ошибки	Статистика ICMP-пакетов и ошибок.
Входящие/исходящие UDP-пакеты и ошибки	Статистика UDP-пакетов и ошибок.
Входящие/исходящие TCP-пакеты и ошибки	Трафик TCP-пакетов и ошибки.
TCP-подключения	Количество активных TCP-подключений (по состояниям).
TCP SynCookie/прямой переход/статистика	Защита файлов cookie с помощью SYN, прямые переходы между состояниями TCP и общая статистика TCP.
Время очистки/очистка Node Exporter	Производительность Node Exporter с акцентом на длительность очистки и требуемый статус.

Настройка уведомлений по электронной почте о событиях работоспособности кластера Kubernetes

Компонент наблюдаемости Kaspersky EDR Expert позволяет уведомлять пользователей по электронной почте о случаях, когда показатели производительности узла кластера Kubernetes превышают нормальные значения. Уведомления по электронной почте создаются на основе соответствующих правил в Grafana. Эти правила определяют содержание уведомлений, получателей и условия отправки уведомлений по электронной почте.

Вы можете просмотреть список доступных правил для уведомлений по электронной почте в Grafana. Можно выбрать предустановленные или пользовательские правила. Предустановленные правила предоставляются Kaspersky EDR Expert, и их невозможно изменить. Пользовательские правила можно создавать, изменять и удалять.

Предустановленные правила отправки уведомлений по электронной почте

Kaspersky EDR Expert включает следующие предустановленные правила отправки уведомлений по электронной почте о событиях работоспособности кластера Kubernetes. Вы не можете удалить или изменить эти правила.

Предустановленные правила отправки уведомлений по электронной почте

Метрика	Уровень важности	Сообщение
High CPU Usage	Предупреждение.	Использование процессора на узле <node_name> превысило ограничение событий предупреждения. Это может указывать на повышенную нагрузку или недостаточность ресурсов процессора.
	Критический	Узел <node_name> испытывает критически высокую загрузку процессора. Это может привести к задержке процессора (англ. CPU throttling), проблемам с расписанием подов- и снижению производительности компонентов кластера.
High Disk I/O Utilization	Предупреждение.	Дисковое устройство <disk_name> на узле <node_name> находится под повышенной нагрузкой ввода/вывода. У приложений может увеличится время отклика.
	Критический	Дисковое устройство <disk_name> на узле <node_name> перегружено. Это может серьезно снизить производительность приложений с отслеживанием статусов.
High Disk Latency	Предупреждение.	Задержка чтения/записи на устройстве хранилища <disk_name> на узле <node_name> превысила ограничение предупреждений.
	Критический	Хранилище <disk_name> на узле <node_name> испытывает критически большую задержку ввода/вывода.
High Disk Usage (Filesystem)	Предупреждение.	Файловая система <mountpoint_name> на узле <node_name> достигла высокого уровня использования. Приближение к ограничению может повлиять на ведение журнала, планирование подов (англ. pod scheduling) или стабильность работы kubelet.
	Критический	Файловая система <mountpoint_name> на узле <node_name> почти заполнена. Это может вызвать ошибки записи, сбои службы и нестабильность узла.
High Memory Usage	Предупреждение.	Использование памяти на узле <node_name> превысило предел событий предупреждения. Рабочие нагрузки могут испытывать нехватку памяти.
	Критический	Узел <node_name> близок к исчерпанию памяти. Это может вызвать OOMKill или выселение подов (pod eviction). Немедленные действия необходимы для предотвращения сбоев рабочей нагрузки.

Чтобы просмотреть стандартные правила отправки уведомлений по электронной почте:

1. Перейдите по URL `<monitoring_host>.<smp_domain>`.

   Где `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры представляют собой FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert. Например: `monitoring.smp.local`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В главном окне приложения перейдите в раздел **Home** → **Alerting** → **Alert rules**.

   В разделе **Alert rules** отображается список предустановленных правил отправки уведомлений по электронной почте.

Пользовательские правила отправки уведомлений по электронной почте

Вы можете создавать правила отправки уведомлений по электронной почте о событиях работоспособности кластера Kubernetes.

> Уведомления по электронной почте не будут отправляться, если параметры подключения к SMTP-серверу не указаны в конфигурационном файле: `grafana_smtp_host`, `grafana_smtp_user`, `grafana_smtp_password`, `grafana_smtp_bundle`, `grafana_smtp_skip_verify`, `grafana_smtp_from_address`, `grafana_smtp_from_name`, `grafana_smtp_ehlo_identity`, `grafana_starttls_policy`, `grafana_smtp_enable_tracing`. Если вы не указали эти параметры в конфигурационном файле перед развертыванием Kaspersky EDR Expert, вы можете добавить их позже.

Чтобы создать пользовательские правила отправки уведомлений по электронной почте:

1. Перейдите по URL `<monitoring_host>.<smp_domain>`.

   Где `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры представляют собой FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert. Например: `monitoring.smp.local`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В главном окне приложения перейдите в раздел **Home** → **Alerting** → **Alert rules**.

4. В разделе **Alert rules** нажмите **New alert rule** и укажите параметры нового правила уведомления по электронной почте.

5. После того как вы укажете параметры правила, нажмите **Save rule and exit**.

   Пользовательское правило создано. Вы также можете создавать папки и размещать в них созданные правила.

Чтобы создать пользовательские правила отправки уведомлений по электронной почте из панели мониторинга:

1. Перейдите по URL `<monitoring_host>.<smp_domain>`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В меню перейдите в раздел **Home** → **Dashboards**.

4. В списке информационных панелей нажмите на имя информационной панели, содержащей индикаторы производительности, которые вы хотите использовать для алертов.

   Откроется панель мониторинга.

5. В интересующей вас панели на панели инструментов нажмите на значок **Меню** (⋮), а затем в контекстном меню выберите **More...** → **New alert rule**.

6. В панели **New alert rule** укажите параметры нового правила уведомлений по электронной почте.

7. Нажмите **Save rule and exit**.

Пользовательское правило создано из панели мониторинга.

Чтобы изменить или удалить пользовательские правила отправки уведомлений по электронной почте:

1. Перейдите по URL `<monitoring_host>.<smp_domain>`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В главном окне приложения перейдите в раздел **Home** → **Alerting** → **Alert rules**.

4. В разделе **Alert rules** найдите нужное правило и выполните одно из следующих действий:

   - Чтобы изменить правило, нажмите на кнопку карандаша и измените параметры правила.

   - Чтобы удалить правило, нажмите **More**, а затем нажмите **Delete**.

Пользовательское правило изменено или удалено.

Управление адресами получателей уведомлений по электронной почте о событиях работоспособности кластера Kubernetes

Kaspersky EDR Expert позволяет задавать, изменять и удалять адреса получателей уведомлений.

> Уведомления по электронной почте не будут отправляться, если параметры подключения к SMTP-серверу не указаны в конфигурационном файле: `grafana_smtp_host`, `grafana_smtp_user`, `grafana_smtp_password`, `grafana_smtp_bundle`, `grafana_smtp_skip_verify`, `grafana_smtp_from_address`, `grafana_smtp_from_name`, `grafana_smtp_ehlo_identity`, `grafana_starttls_policy`, `grafana_smtp_enable_tracing`. Если вы не указали эти параметры в конфигурационном файле перед развертыванием Kaspersky EDR Expert, вы можете добавить их позже.

Чтобы добавить адрес электронной почты получателей уведомлений:

1. Перейдите по веб-адресу `<monitoring_host>.<smp_domain>`.

   Где `<monitoring_host>` – имя устройства, `<smp_domain>` – имя домена. Эти параметры представляют собой FQDN службы мониторинга Kaspersky EDR Expert и определяются в конфигурационном файле при развертывании Kaspersky EDR Expert. Например: `monitoring.smp.local`.

2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

3. В главном окне приложения перейдите в раздел **Home** → **Alerting** → **Contact points**.

4. В рабочей области **Contact points** нажмите **Add contact point** и укажите следующие параметры получателя:

   - **Name** – имя получателя или группы получателей. Обязательное поле.
   - **Integration** – тип интеграции. Используйте значение Email для уведомления по электронной почте.
   - **Addresses** – один или несколько адресов электронной почты получателей. Адреса могут быть разделены запятой, переводом строки (`\n`) или точкой с запятой.
   - **Single email** – возможность отправить одно электронное письмо всем получателям. Возможные значения параметра:
     - **Enabled** – все получатели получают одно уведомление по электронной почте.
     - **Disabled** – каждый получатель получает отдельное уведомление по электронной почте.
   - **Message** – тело письма. Вы можете использовать шаблоны или задать собственный текст, нажав на кнопку **Edit Message**.
   - **Subject** – тема электронного письма. Вы можете использовать шаблоны или указать свою тему письма, нажав на кнопку **Edit Subject**.
   - **Notification settings** – общие параметры уведомлений.
   - **Disable resolved message** – выключает отправку сообщения при устранении проблемы или алерта.
   - **Test** – отправка тестового уведомления. Позволяет проверить правильность настроенных параметров.
   - **Duplicate** – создание копии конфигурации точки контакта. Позволяет быстро создавать похожие точки контакта.
   - **Delete** – удаление текущей конфигурации точки контакта.

5. Нажмите на **Save contact point**.

Чтобы изменить или удалить адреса получателей уведомлений:

1. Перейдите по веб-адресу `<monitoring_host>.<smp_domain>`.
2. Введите учетные данные Grafana, которые вы указали в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).
3. В главном окне приложения перейдите в раздел **Home** → **Alerting** → **Contact points**.
4. В рабочей области **Contact points** найдите нужный контакт и выполните одно из следующих действий:
   - Чтобы изменить правило, нажмите на кнопку карандаша и измените параметры правила.
   - Чтобы удалить правило, нажмите **More**, а затем нажмите **Delete**.

Контакт изменен или удален.

Добавление параметров подключения к SMTP-серверу в конфигурационный файл без переустановки Kaspersky EDR Expert

Чтобы добавить параметры подключения к SMTP-серверу в конфигурационный файл без переустановки Kaspersky EDR Expert:

1. На устройстве администратора выполните экспорт текущей версии конфигурационного файла.

2. В экспортированном конфигурационном файле добавьте и укажите следующие секции `parameters`: `grafana_smtp_host`, `grafana_smtp_user`, `grafana_smtp_password`, `grafana_smtp_bundle`, `grafana_smtp_skip_verify`, `grafana_smtp_from_address`, `grafana_smtp_from_name`, `grafana_smtp_ehlo_identity`, `grafana_starttls_policy`, `grafana_smtp_enable_tracing`.

3. Примените изменения параметров с помощью команды:

   ```
   ./kdt apply -i '< полный_путь_к_обновленному_конфигурационному_файлу >'
   ```

Параметры подключения к SMTP-серверу добавлены в конфигурационный файл.

Мониторинг сервисов

Вы можете использовать следующие возможности, чтобы отслеживать состояние всех сервисов, кроме холодного хранилища и агента:

- Просматривать алерты VictoriaMetrics.

  Пользователи с ролью Главный администратор могут настраивать пороговые значения параметров сервисов KUMA и если заданные пороговые значения будут превышены, произойдут следующие изменения:

  - KUMA зарегистрирует событие аудита Зарегистрирован алерт Victoria Metrics для сервиса.

  - KUMA отправит уведомление Главному администратору по электронной почте.

  - Сервисы будут отображаться в разделе **Активные сервисы** в желтом статусе. Если вы наведете курсор на значок статуса, сообщение об ошибке будет доступно для просмотра.

    Доступные статусы сервисов

    - Зеленый – сервис работает и доступен с сервера Ядра KUMA.

    - Красный – сервис не работает или не доступен с сервера Ядра KUMA.

    - Желтый – сервис работает, но в журнале сервиса есть ошибки или для сервиса есть алерты от Victoria Metrics. Сообщение об ошибке отображается, если навести курсор мыши на статус сервиса. Желтый статус применяется ко всем сервисам, кроме агента.

- Фиолетовый – изменился конфигурационный файл сервиса, но другие ошибки отсутствуют. Если у сервиса некорректный конфигурационный файл и есть ошибки, например от Victoria Metrics, статус сервиса будет желтым.

- Серый – в удаленном тенанте был работающий сервис, который продолжает работать. Сервисы в сером статусе остаются после удаления тенанта, чтобы вы могли скопировать идентификатор и удалить сервисы на серверах. Удалить сервисы с серым статусом может только Главный администратор. При удалении тенанта сервисы этого тенанта привязываются к тенанту Main.

- Просматривать метрики VictoriaMetrics при условии наличия у пользователя роли с правами доступа к метрикам.

В следующих примерах показано, каким образом вы можете отслеживать состояние сервисов.

1. Если в разделе **Активные сервисы** сервис коллектора находится в желтом статусе и есть сообщение **Enrichment errors increasing**, вы можете выполнить следующие действия:

   - Перейти в раздел **Мониторинг** → **Метрики** → <тип сервиса> → <имя сервиса> → **Enrichment** → **Errors** для сервиса в желтом статусе, выяснить, какое именно обогащение работает с ошибками, и просмотреть график, чтобы уточнить когда именно началась проблема и отследить динамику.

   - Поскольку вероятной причиной ошибок обогащения может быть недоступность DNS-сервера или ошибки обогащения CyberTrace, вы можете проверить параметры подключения DNS или CyberTrace.

2. Если в разделе **Активные сервисы** сервис коллектора находится в желтом статусе и есть сообщение **Output Event Loss increasing**, вы можете выполнить следующие действия:

   - Перейдите в раздел **Мониторинг** → **Метрики** → <тип сервиса> → <имя сервиса> → **IO** → **Output Event Loss** для сервиса в желтом статусе и просмотрите график, чтобы определить, когда началась проблема, и отследите динамику.

   - Поскольку вероятной причиной потери событий может быть превышение размера буфера или недоступность точки назначения, вы можете проверить доступность и правильность подключения точки назначения или выяснить, почему превышен размер буфера.

Настройка параметров мониторинга сервисов

Чтобы настроить параметры сервисов:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке Другое нажмите **Мониторинг сервисов**.

   Откроется окно **Мониторинг сервисов**.

3. Укажите значения параметров мониторинга для сервисов.

   Мониторинг сервисов не распространяется на холодное хранилище.

   Если вы указали некорректное значение, которое не подходит по диапазону или формату, значение будет сброшено до ранее установленного.

4. Нажмите **Сохранить**.

   После сохранения параметров KUMA регистрирует аудит событие Пороговые значение параметров мониторинга сервисов изменены.

KUMA отслеживает состояние сервисов по заданным параметрам.

В разделе **Активные сервисы** вы можете отфильтровать сервисы по статусам или указать в поле поиска слово из текста ошибки, например "QPS" или "buffer", и нажать ENTER. В результате отобразится список сервисов с ошибками. Не используйте в поле поиска специальные символы ", }, {. В этом случае результаты поиска будут неактуальные.

Отключение мониторинга сервисов

Чтобы отключить мониторинг сервисов:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке Другое нажмите **Мониторинг сервисов**.

   Откроется окно **Мониторинг сервисов**.

3. Если вы хотите отключить мониторинг сервисов только для коллекторов, в окне **Мониторинг сервисов. Настройка пороговых значений** в блоке параметров **Коллекторы** установите флажок **Отключить ошибки коннекторов**.

   В результате будет отключен только анализ метрики **Connector errors** для коллекторов.

4. Если вы хотите отключить мониторинг всех сервисов, в окне **Мониторинг сервисов. Настройка пороговых значений** установите флажок **Выключить**.

Мониторинг сервисов KUMA будет отключен, при этом сервисам не будет присваиваться желтый статус.

Просмотр метрик KUMA

Для отслеживания работы своих компонентов, потока событий, контекста корреляции в KUMA выполняется сбор и хранение большого количества параметров. Для сбора, хранения и анализа параметров используется решение VictoriaMetrics, представляющее собой СУБД в формате временных рядов. Полученные метрики можно просматривать с помощью Grafana. В разделе **Мониторинг** → **Метрики** представлены панели мониторинга с визуализацией ключевых параметров работы различных компонентов KUMA.
Сервис Ядра KUMA выполняет настройку параметров VictoriaMetrics и Grafana автоматически, участие пользователя не требуется.

Также метрики KUMA можно просмотреть в разделе **Панель мониторинга**:

1. В главном меню перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Нажмите на значок с многоточием (⋮).

3. Нажмите на кнопку **Перейти к метрикам KUMA**.

Полученные метрики можно просматривать с помощью решения Grafana. RPM-пакет службы kuma-core генерирует конфигурацию Grafana и создает отдельную панель мониторинга для визуализации показателей каждой службы. Графики в разделе **Метрики** появляются с задержкой примерно в 1,5 минуты.

Полную информацию о метриках вы можете найти в Консоли OSMP в разделе **Показатели**. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA. Если в разделе **Метрики** вы видите core: <номер порта>, это означает, что KUMA развернута в отказоустойчивой конфигурации и метрики получены с устройства, на котором было **установлено Ядро**. В прочих конфигурациях отображается имя устройства, с которого KUMA получает метрики.

Чтобы определить, на каком устройстве работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

Метрики коллектора

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.
Write Network BPS	Количество байт, принятых в сеть за секунду.
Connector errors	Количество ошибок в журналах событий коннектора.

Normalization (Нормализация) – показатели, относящиеся к нормализаторам.	
Raw & Normalized event size	Размер сырого события и размер нормализованного события. Отображается среднее значение.
Errors	Количество ошибок нормализации в секунду.

Filtration – показатели, относящиеся к фильтрам.	
EPS	Количество событий, удовлетворяющих условиям фильтра и отправленных в обработку в секунду. Коллектор обрабатывает события, удовлетворяющие условиям фильтра, только если пользователь добавил фильтр в конфигурацию службы коллектора.

Aggregation (Агрегация) – показатели, относящиеся к правилам агрегации.	
EPS	Количество событий, полученных и созданных правилом агрегации в секунду. Этот показатель помогает определить эффективность правил агрегации.
Buckets	Количество контейнеров в правиле агрегации.

Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.
Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.

Показатели корреляторов

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.

Correlation – показатели, относящиеся к правилам корреляции.	
EPS	Количество событий корреляции в секунду, созданных правилом корреляции.
Buckets	Количество контейнеров в правиле корреляции стандартного типа.
Rate Limiter Hits	Количество превышений правилом корреляции предельного значения срабатываний в секунду.
Active Lists OPS	Количество запросов на выполнение операций, отправленных активному листу в секунду, и сами операции.

Active Lists Records	Количество записей в активном листе.
Active Lists On-Disk Size	Размер активного листа на диске в байтах.

Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.
Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.

Response – показатели, связанные с правилами реагирования.	
RPS	Количество срабатываний правила реагирования в секунду.

Метрики хранилища

Название метрики	Описание
ClickHouse/General – показатели, относящиеся к общим параметрам кластера ClickHouse.	
Active Queries	Количество активных запросов, отправленных кластеру ClickHouse. Эта метрика отображается для каждого экземпляра ClickHouse.
QPS	Количество запросов в секунду, отправленных кластеру ClickHouse.
Failed QPS	Количество неудачных запросов в секунду, отправленных кластеру ClickHouse.
Allocated memory	Объем оперативной памяти в гигабайтах, выделенной процессу ClickHouse.

ClickHouse/Insert – метрики, относящиеся к вставке событий в экземпляр ClickHouse.	
Insert EPS	Количество событий в секунду, вставленных в экземпляр ClickHouse.

Insert QPS	Количество запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Если на метрике **Insert QPS** растет очередь из запросов и показатель превышает 1, рекомендуется посмотреть также значение метрики **Batch size**, чтобы скорректировать параметры буферизации хранилища в параметрах конфигурации службы хранилища. Пример: Показатель метрики **Insert QPS** превышает 1 и равен 8. Показатель **Batch size** – 1,2 ГБ (в байтах). В этом случае следует определить размер буфера, перемножив показатели метрик **Insert QPS** и **Batch size**: 8 * 1.2 = 9.6 ГБ. Полученное значение 9.6 следует округлить и указать в байтах (например, 10000000000 байт) в качестве значения параметра **Размер буфера** на вкладке **Дополнительные параметры** в настройках конфигурации сервиса хранилища. Также следует указать значение параметра **Интервал очистки буфера** – 2 с. Увеличение размера буфера и интервала очистки буфера позволит разгрузить очередь запросов. При нормальных условиях показатель метрики **Insert QPS** не превышает 1.
Failed Insert QPS	Количество неудачных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse.
Delayed Insert QPS	Количество отложенных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения мягкого ограничения активного объединения запросов.
Rejected Insert QPS	Количество отклоненных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения жесткого ограничения активного объединения запросов.
Active Merges	Количество активных объединений запросов.
Distribution Queue	Количество временных файлов с событиями, которые не удалось вставить в экземпляр ClickHouse из-за его недоступности. Эти события не могут быть найдены с помощью поиска.

ClickHouse/Select – показатели, относящиеся к выборкам событий в экземпляре ClickHouse.	
Select QPS	Количество запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.
Failed Select QPS	Количество неудачных запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.

ClickHouse/Replication – метрики, относящиеся к репликам узлов ClickHouse.	
Active Zookeeper Connections	Количество активных подключений к узлам кластера Zookeeper. При нормальной работе это количество должно быть равно количеству узлов в кластере Zookeeper.
Read-only Replicas	Количество реплик узлов ClickHouse, доступных только для чтения. При нормальной работе таких реплик узлов ClickHouse нет.
Active Replication Fetches	Количество активных процессов скачивания данных с узла ClickHouse при репликации данных.
Active Replication Sends	Количество активных процессов отправки данных узлу ClickHouse при репликации данных.
Active Replication Consistency Checks	Количество активных проверок согласованности данных на репликах узлов ClickHouse при репликации данных.

ClickHouse/Networking – показатели, относящиеся к сети кластера ClickHouse.	
Active HTTP Connections	Количество активных подключений к HTTP-серверу кластера ClickHouse.

Active TCP Connections	Количество активных подключений к TCP-серверу кластера ClickHouse.
Active Interserver Connections	Количество активных межсервисных соединений между узлами ClickHouse.

Показатели Ядра KUMA

Название метрики	Описание
Raft – метрики, связанные с чтением и обновлением состояния Ядра KUMA.	
Lookup RPS	Количество запросов процедуры поиска в секунду, отправленных в Ядро KUMA, и сами процедуры.
Lookup Latency	Время в миллисекундах, затраченное на выполнение процедур поиска и на выполнение самих процедур. Отображается время для 99-го процентиля процедур поиска. Один процент процедур поиска может занять больше времени.
Propose RPS	Количество запросов на выполнение процедур обновления состояния Raft (SQLite), отправленных Ядру в секунду, и сами процедуры.
Propose Latency	Время в миллисекундах, затраченное на выполнение процедур обновления состояния Raft (SQLite), и сами процедуры. Отображается время для 99-го процентиля процедур обновления состояния. Один процент процедур обновления состояния может занять больше времени.
Data mining – метрики, относящиеся к сбору и анализу данных	
Executing Rules	Количество запущенных планировщиков для выполнения запросов сбора и анализа данных.
Queued Rules	Количество планировщиков для выполнения запросов сбора и анализа данных в очереди.
Execution Errors	Количество ошибок при выполнении запуска планировщика сбора и анализа данных.
Execution Latency	Время выполнения запросов планировщика.
Tasks – метрики, относящиеся к мониторингу выполнения задач на Ядре KUMA	
Active tasks	Количество выполняемых задач за единицу времени.
Task Execution latency	Время выполняемых задач в секундах.
Errors	Количество ошибок при выполнении задач.

API – метрики, относящиеся к запросам API.	
RPS	Количество запросов API к Ядру KUMA в секунду.
Latency	Время в миллисекундах, затраченное на обработку одного запроса API к Ядру KUMA. Отображается среднее значение.
Errors	Количество ошибок в секунду при отправке API-запросов к Ядру KUMA.

Notification Feed – показатели, относящиеся к активности пользователей.	
Subscriptions	Количество клиентов, подключенных к Ядру KUMA через SSE для получения сообщений сервера в реальном времени. Это число обычно равно количеству клиентов, использующих Консоль KUMA.
Errors	Количество ошибок в секунду при отправке уведомлений пользователям.

Schedulers – показатели, относящиеся к задачам Ядра KUMA.	
Активная	Количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
Latency	Время в миллисекундах, затраченное на выполнение задачи. Отображается среднее значение.
Errors	Количество ошибок в секунду, возникших при выполнении задач.

Метрики, общие для всех сервисов

Название метрики	Описание
Process – общие метрики процесса.	
Memory	Использование оперативной памяти (RSS) в мегабайтах.
DISK BPS	Количество байтов, считываемых с диска или записываемых на диск в секунду.
Network BPS	Количество байтов, получаемых/передаваемых в сеть в секунду.
Network Packet Loss	Количество сетевых пакетов, потерянных в секунду.
GC Latency	Время в миллисекундах, затраченное на выполнение цикла сборщика мусора GO (Garbage Collector). Отображается среднее значение.
Goroutines	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS – показатели, относящиеся к операционной системе.	
Load	Средняя нагрузка.
Процессор	Загрузка процессора в процентах.
Memory	Использование оперативной памяти (RSS) в процентах.
Disk	Использование дискового пространства в процентах.

Срок хранения метрик

По умолчанию данные о работе KUMA хранятся 3 месяца. Этот срок можно изменить.

Чтобы изменить срок хранения метрик KUMA:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service в параметре ExecStart измените флаг `--retentionPeriod=<срок хранения метрик в месяцах>`, подставив нужный срок. Например, `--retentionPeriod=4` означает, что метрики будут храниться 4 месяца.

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-victoria-metrics`

Срок хранения метрик изменен.

Условия срабатывания алертов по метрикам KUMA

Если значение метрики KUMA о работе сервиса превышает пороговое значение соответствующего параметра, настроенного в разделе KUMA **Мониторинг сервисов**, от решения VictoriaMetrics поступает алерт, и в статусе этого сервиса отображается сообщение об ошибке.

Получение алертов от VictoriaMetrics происходит со следующей периодичностью:

- VictoriaMetrics получает информацию от сервисов KUMA каждые 15 секунд.
- VictoriaMetrics обновляет алерты для сервисов KUMA каждую минуту.
- Сервис Ядро KUMA получает информацию от VictoriaMetrics каждые 15 секунд.

Таким образом время требуемое для обновления статуса сервиса может достигать не более 2–3 минут.

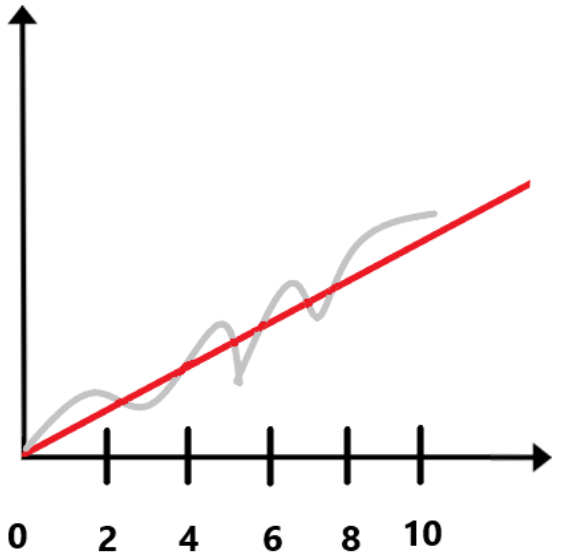
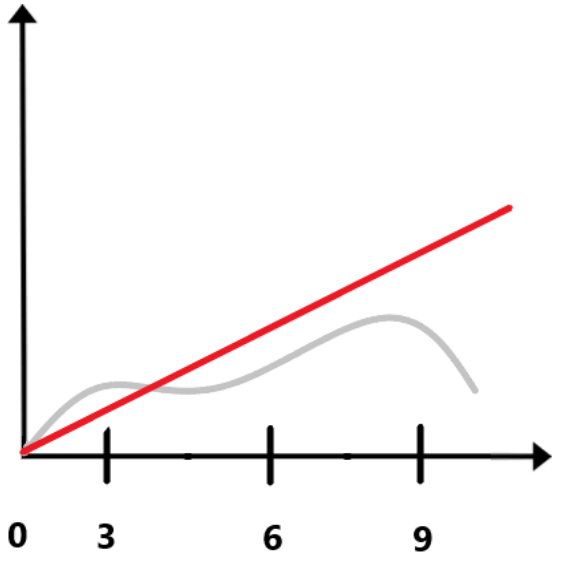
Если вы выключили получение алертов от VictoriaMetrics, некоторые сервисы KUMA все равно могут отображаться с желтым статусом. Это может произойти в следующих случаях:

- Для сервиса хранилище:
  - если алерт был получен в результате API-запроса в параметре /status от ClickHouse;
  - если холодное хранилище сервиса Хранилище не проверяется.
- Для сервиса коллектор: если алерт был получен в результате API-запроса в параметре /status.
- Для сервиса коррелятор: если есть правило реагирования, для которого требуется модуль Advanced Responses, но этот модуль отсутствует в действующей лицензии или срок действия лицензии, в которой есть этот модуль, истек.

В таблице ниже представлена информация о том, какие сообщения об ошибке могут появиться в статусе сервиса при получении алерта от VictoriaMetrics и как и на основании каких метрик и параметров они рассчитываются. Подробнее о метриках KUMA, на основании которых могут быть созданы алерты VictoriaMetrics, см. Просмотр метрик KUMA.

Например, если в таблице **Активные сервисы** для сервиса отображается желтый статус и сообщение об ошибке `High distribution queue` (в таблице ниже – столбец "Сообщение об ошибке"), вы можете посмотреть данные в виджете **Enrichment**, метрика **Distribution Queue** (в таблице ниже – столбец "Метрики KUMA").

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика KUMA	Описание
`QPS threshold reached`	**Интервал/Окно QPS, минуты** **Порог QPS**	Clickhouse / General (общие параметры) → Failed QPS (безуспешные запросы в секунду)	Сообщение об ошибке отображается, если значение метрики Failed QPS превышает заданное значение параметра **Порог QPS** в течение интервала времени, заданного параметром **Интервал/Окно QPS, минуты**. Например, если из 100 запросов от решения VictoriaMetrics к сервису 25 пришли безуспешные, а параметр **Порог QPS** равен 0.2, алерт рассчитывается следующим образом: (25 / 100) * 100 > 0.2 * 100 25% > 20% Так как процент безуспешных запросов больше, чем заданный порог, для сервиса отобразится сообщение об ошибке.
`Failed Insert QPS threshold reached`	**Интервал/Окно расчета ошибочных вставок QPS, минуты** **Порог вставок QPS**	Clickhouse / Insert (вставка) → Failed Insert QPS (безуспешные запросы на вставку в секунду)	Сообщение об ошибке отображается, если значение метрики Failed Insert QPS превышает заданное значение параметра **Порог вставок QPS** в течение интервала времени, заданного параметром **Интервал/Окно расчета ошибочных вставок QPS, минуты**. Например, если из 100 запросов от решения VictoriaMetrics к сервису 25 пришли безуспешные, а параметр **Порог вставок QPS** равен 0.2, алерт рассчитывается следующим образом: (25 / 100) * 100 > 0.2 * 100 25% > 20% Так как процент безуспешных запросов больше, чем заданный порог, для сервиса отобразится сообщение об ошибке.
`High distribution queue`	**Порог очереди распределения** **Интервал/Окно расчета очереди распределения, минуты**	Clickhouse / Insert (вставка) → Distribution Queue (очередь распределения)	Сообщение об ошибке отображается, если значение метрики Distribution Queue превышает заданное значение параметра **Порог очереди распределения** в течение интервала времени, заданного параметром **Интервал/Окно расчета очереди распределения, минуты**.
`Low disk space`	**Порог свободного места на диске**	OS (ОС) → Disk (диск)	Сообщение об ошибке отображается, если размер свободного места на диске (в процентах) в значении метрики Disk меньше, чем задано в параметре **Порог свободного места на диске**. Например, сообщение об ошибке отобразится, если раздел диска, на котором установлено решение KUMA, занимает все место на диске.
`Low disk partition space`	**Порог свободного места на разделе диска**	OS (ОС) → Disk (диск)	Сообщение об ошибке отображается, если размер свободного места в разделе диска, с которым работает KUMA (в процентах), осталось меньше, чем задано в параметре **Порог свободного места на разделе диска**. Например, сообщение об ошибке отобразится в следующих случаях: • При установке KUMA в отказоустойчивой конфигурации, когда диск подключается как том. • Если диск монтирован в раздел /opt.
`Output Event Loss increasing`	**Потери исходящих событий**	IO (ввод/вывод) → Output Event Loss (потеря событий)	Сообщение об ошибке отображается, если значение метрики Output Event Loss возрастает в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Потери исходящих событий**.

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика KUMA	Описание
`Disk buffer size increasing`	**Интервал/Окно увеличения дискового буфера, минуты**	IO (ввод/вывод) → Output Disk Buffer Size (размер дискового буфера)	Сообщение об ошибке отображается, если в течение 10 минут с интервалом, заданным параметром **Интервал/Окно увеличения дискового буфера, минуты**, значение метрики Output Disk Buffer Size монотонно возрастает. Например, при значении параметра **Интервал/Окно увеличения дискового буфера, минуты** равном 2 минуты сообщение об ошибке отобразится, если в течение 10 минут размер дискового буфера будет монотонно возрастать каждые 2 минуты (см. рис. ниже). 
`High enrichment queue`	**Интервал/Окно увеличения очереди обогащения, минуты**	Enrichment (обогащение) → Queue (очередь)	Сообщение об ошибке отображается, если в течение 10 минут с интервалом, заданным параметром **Интервал/Окно увеличения очереди обогащения, минуты**, значение метрики Queue монотонно возрастает. Например, при значении параметра **Интервал/Окно увеличения очереди обогащения, минуты** равном 3 минуты сообщение об ошибке отобразится, если в течение 10 минут очередь обогащения будет монотонно возрастать каждые три минуты. В случае, изображенном на рисунке ниже, сообщение об ошибке не отобразится, так как на девятой минуте значение метрики уменьшилось, поэтому последовательного монотонного возрастания нет. 

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика KUMA	Описание
`Enrichment errors increasing`	**Ошибки обогащения**	Enrichment (обогащение) → Errors (ошибки)	Сообщение об ошибке отображается, если значение метрики Errors (количество ошибок) возрастает в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Ошибки обогащения**.
`Connector log errors increasing`	**Отключить ошибки коннекторов**	IO (ввод/вывод) → Connector Errors (ошибки коннектора)	Сообщение об ошибке отображается, если значение метрики Connector Errors (количество ошибок) возрастает между последовательными опросами метрики решением VictoriaMetrics в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Отключить ошибки коннекторов**.

Хранение диагностической информации о компонентах Kaspersky EDR Expert

Диагностическая информация о компонентах Kaspersky EDR Expert хранится на рабочем узле кластера Kubernetes. Объем дискового пространства, необходимый для хранения этой информации, указывается в конфигурационном файле перед развертыванием Kaspersky EDR Expert (параметр `loki_size`).

Чтобы проверить объем дискового пространства, на котором хранится диагностическая информация о компонентах Kaspersky EDR Expert,

на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke observability --action getPvSize
```

Отображается объем выделенного свободного места на диске в гигабайтах.

Вы также можете увеличить дисковое пространство, используемое для хранения диагностической информации о компонентах Kaspersky EDR Expert после установки Kaspersky EDR Expert. Вы не можете установить объем дискового пространства меньше указанного ранее.

Чтобы увеличить дисковое пространство, используемое для хранения диагностической информации о компонентах Kaspersky EDR Expert,

на устройстве администратора, на котором расположена утилита KDT, выполните команду, указав необходимое свободное место на диске в гигабайтах (например, "50Gi"):

```
./kdt invoke observability --action setPvSize --param
loki_size='<новый_объем_дискового_пространства>Gi'
```

Объем свободного дискового пространства, выделяемого для хранения диагностической информации о компонентах Kaspersky EDR Expert, изменен.

Получение файлов трассировки

KDT позволяет получать файлы трассировки для Kaspersky EDR Expert и компонентов OSMP, чтобы устранять проблемы инфраструктуры самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Файлы трассировки загружаются в формате OpenTelemetry.

Чтобы получить файл трассировки для Kaspersky EDR Expert или компонента OSMP:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите путь к файлу, в который вы хотите сохранить список файлов трассировки:

   ```
   ./kdt traces find -o <output_file_path>
   ```

   Список файлов трассировки с их идентификаторами выводится в указанный файл.

2. Чтобы вывести конкретный файл трассировки, выполните следующую команду и укажите путь к выходному файлу и идентификатор файла трассировки:

   ```
   ./kdt traces get -o <output_file_path> --trace-id=<trace_ID>
   ```

Указанный файл трассировки сохранен.

Запись событий запусков пользовательских действий

KDT позволяет получить историю запуска пользовательского действия для конкретного компонента Kaspersky EDR Expert, а также журналы событий запуска определенного пользовательского действия. Полученные журналы событий могут помочь вам исследовать проблемы с работой компонентов Kaspersky EDR Expert самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Чтобы получить историю запусков пользовательских действий для конкретного компонента Kaspersky EDR Expert:

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента:

```
./kdt state -H <component_name>
```

Отображается список выполненных пользовательских действий с их идентификаторами.

Чтобы получить журналы событий запуска настраиваемого действия,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента и идентификатор запуска пользовательского действия:

```
./kdt state -l <component_name> -m <custom_action_launch_ID>
```

Отобразятся журналы событий запуска указанного пользовательского действия.

Управление пользователями и ролями пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

Об учетных записях пользователей

Kaspersky EDR Expert позволяет управлять учетными записями пользователей и группами безопасности. Приложение поддерживает четыре типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих доменных пользователей при опросе контроллеров доменов организации.
- Учетные записи локальных пользователей. Локальные учетные записи управляемых устройств, а также локальные учетные записи устройства, на котором установлен Сервер администрирования.
- Учетные записи внутренних пользователей Kaspersky EDR Expert. Вы можете создавать учетные записи внутренних пользователей. Эти учетные записи используются только в Kaspersky EDR Expert.
- Учетные записи служб. Эти учетные записи используются только для подключения служб Kaspersky EDR Expert к Серверу администрирования. Учетные записи служб добавляются автоматически при развертывании решения, и их невозможно удалить или изменить. Права и роли этих учетных записей также невозможно изменить. Вы не можете использовать учетную запись службы для входа в Консоль OSMP.

Учетные записи локальных пользователей и локальная группа kladmins в операционной системе Linux не могут быть использованы для доступа к OSMP Console в Open Single Management Platform. Группа kladmins может содержать только учетные записи, которые используются для запуска служб Open Single Management Platform. Использование учетных записей сотрудников организации для входа становится доступно после настройки доменной аутентификации.

Метод аутентификации по умолчанию в Консоли OSMP заключается в вводе имени пользователя, пароля и дополнительного одноразового кода безопасности для двухфакторной аутентификации. Начиная с Kaspersky EDR Expert версии 2.0, двухфакторная аутентификация включается автоматически, а возможность настраивать двухфакторную аутентификацию при входе в систему выключена по умолчанию.

Вы можете настроить доменную аутентификацию по протоколу Kerberos. Доменная аутентификация позволяет вам включить безопасную аутентификацию в Консоли OSMP без повторного ввода пароля в корпоративной сети (единый вход).

Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. Перейдите на вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности.

Если вы хотите просмотреть таблицу только с внутренними, локальными или доменными пользователями или группами, установите в фильтре для критерия **Тип учетной записи** соответствующее значение.

Если таблица пользователей содержит более 50 000 пользователей, отображаются только первые 50 000 пользователей, остальные пользователи не отображаются.

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами приложениями "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов.

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования.

Область роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Преимущество использования ролей

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных служебных обязанностей, требующих разных параметров безопасности, значительно меньше.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

Настройка прав доступа к функциям приложения. Управление доступом на основе ролей

Kaspersky EDR Expert предоставляет доступ на основе ролей к функциям Kaspersky EDR Expert и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Kaspersky EDR Expert одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложение можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права.

Права доступа к функциям приложения

В таблице ниже приведены функции Kaspersky EDR Expert с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Управление группами администрирования**	**Запись.**	• Добавление устройства в группу администрирования: **Запись**. • Удаление устройства из состава группы администрирования: **Запись**. • Добавление группы администрирования в другую группу администрирования: **Запись**. • Удаление группы администрирования из другой группы администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение.**	Получение доступа на чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	Фун обла **фун** **к об** **неза** **спис** пред для поль пред прав этой фун обла полу дост ко в Реко пред прав огра круг поль кото нуж выпо служ обяз Дос пред неза друг если запр дост опре объ
Общие функции: **Базовая функциональность**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**. • Получение мобильного протокола (LWNGT) пользовательского сертификата: **Чтение**. • Установка мобильного протокола (LWNGT) пользовательского сертификата: **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об инцидентах. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Просмотр списка контроля доступа групп: **Чтение**. • Просмотр журнала операционной системы: **Чтение**.		• Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет о правах доступа к зашифрованным дискам. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: **Удаленные объекты**	• **Чтение.** • **Запись.**	• Просмотр удаленных объектов в корзине: **Чтение**. • Удаление объектов из корзины: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Обработка событий**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Запись.**	• Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий**. • Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях**. • Удаление событий: **Удаление событий**.	Отсутствует.	Отсутствует.	Пара • •
Общие функции: **Операции с Сервером администрирования**	• **Чтение.** • **Запись.** • **Выполнение.** • **Изменение списков ACL объекта.** • **Выполнение действий над выборками устройств.**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись**.	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**. • Изменение SSL-портов Сервера администрирования для подключения с помощью Консоли OSMP: **Запись**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.			
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях.	Инст паке "Лаб Касп

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	
Общие функции: **Управление лицензионными ключами**	• **Экспорт файл ключа.** • **Запись.**	• Экспорт файл ключа: **Экспорт файл ключа.** • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Управление отчетами**	• **Чтение.** • **Запись.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • Выполнять отчеты независимо от их списков ACLs: **Чтение**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Иерархия Серверов администрирования**	**Настройка иерархии Серверов администрирования**	• Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Права пользователя**	**Изменение списков ACL объекта.**	• Изменение свойств Безопасности любого объекта: **Изменение списков ACL объекта**. • Управление ролями пользователей: **Изменение списков ACL объекта**. • Управление внутренними пользователями: **Изменение списков ACL объекта**. • Управление группами безопасности: **Изменение списков ACL объекта**. • Управление псевдонимами: **Изменение списков ACL объекта**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Виртуальные Серверы администрирования**	• **Управление виртуальными Серверами администрирования.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение списка виртуальных Серверов администрирования: **Чтение**. • Получение информации о виртуальном Сервере администрирования: **Чтение**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования**. • Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами администрирования**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования**.			
Общие функции: **Управление ключами шифрования**	**Запись.**	Подтверждение запуска плейбука в обучающем режиме: **Запись**.	Отсутствует.	Отсутствует.	Отс
Управление системой: **Системное администрирование**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр свойства патчей сторонних производителей: **Чтение**. • Изменение свойства патчей сторонних производителей: **Запись**.	• Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отс

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky EDR Expert, предоставляют им набор прав доступа к функциям приложения.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных пользовательских ролей, доступных в Kaspersky EDR Expert, можно связать с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер**. Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

Примеры ролей для определенных должностей

Роль	Описание
Аудитор	Разрешает выполнение всех операций со всеми типами отчетов и всех операций просмотра, включая просмотр удаленных объектов (предоставляет права **Чтение** и **Запись** в области **Удаленные объекты**). Не разрешает выполнять другие операции. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.

Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Специалист по безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Права предопределенных ролей пользователей

Роль	Описание
Основные роли	

Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность**
	  • **Управление ключами шифрования**
	  • **Обработка событий**
	  • **Иерархия Серверов администрирования**
	  • **Виртуальные Серверы администрирования**
	• **Управление системой**:
	  • **Подключения**
	  • **Инвентаризация оборудования**
	  • **Инвентаризация приложений**

Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность**
	  • **Управление ключами шифрования**
	  • **Виртуальные Серверы администрирования**
	• **Управление системой**:
	  • **Подключения**
	  • **Инвентаризация оборудования**
	  • **Инвентаризация приложений**

Аудитор	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL** • **Удаленные объекты** • **Управление отчетами** Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Базовая функциональность** • **Развертывание приложений "Лаборатории Касперского"** • **Управление лицензионными ключами** Предоставляет права на **Чтение** и **Выполнение** в следующей функциональной области **Базовая функциональность: Виртуальные Серверы администрирования**.
Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общие функции**: • **Базовая функциональность** • **Развертывание приложений "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области) • **Виртуальные Серверы администрирования**
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность** • Область Kaspersky Endpoint Security, включая все функции Предоставляет права на **Чтение** и **Запись** в области **Общие функции: Управление ключами шифрования**.

Роль	Описание
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: • **Общие функции: Базовая функциональность** • Область Kaspersky Endpoint Security, включая все функции
Главный администратор	Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общие функции**: • **Доступ к объектам независимо от их списков ACL** • **Управление отчетами** Предоставляет права на **Чтение** и **Запись** в области **Общие функции: Управление ключами шифрования**.
Главный оператор	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях: • **Общие функции**: • **Базовая функциональность** • **Удаленные объекты** • **Операции с Сервером администрирования** • **Развертывание приложений "Лаборатории Касперского"** • **Виртуальные Серверы администрирования** • Область Kaspersky Endpoint Security, включая все функции.
Администратор управления мобильными устройствами	Разрешает все операции в области **Общие функции: функциональная область Базовая функциональность**.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL** • **Управление отчетами** Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочую станцию администратора** и **Выполнение операций с выборками устройств** в области **Управление системой: Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.
Пользователь Self Service Portal	Разрешает все операции в области **Управление мобильными устройствами: Self Service Portal**. Эта функция не поддерживается в версиях приложения Kaspersky Security Center 11 и выше.
Контролер	Предоставляет права на **Чтение** в области **Общие функции**: **Доступ к объектам независимо от их списков ACL** и **Общие функции**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
EDR-роли	
Главный администратор	Разрешает все операции в функциональных областях EDR: • **Алерты и инциденты** • **Detection and response** • **Плейбуки и действия по реагированию** • **Управление активами** • **IAM** • **Тенанты** • **Интеграция с приложениями "Лаборатории Касперского"** • **Интеграция с приложениями сторонних производителей** • **Лицензии**
Администратор тенанта	Разрешает все операции в функциональных областях EDR: • **Алерты и инциденты** • **Detection and response** • **Плейбуки и действия по реагированию** • **Управление активами** • **IAM** • **Тенанты** • **Интеграция с приложениями "Лаборатории Касперского"** • **Интеграция с приложениями сторонних производителей** • **Лицензии** Эта роль соответствует роли Главного администратора, но имеет ограничение. В KUMA администратор тенанта имеет ограниченный доступ к предустановленным объектам.

Роль	Описание
Администратор SOC	Предоставляет следующие права в функциональных областях EDR: • **Detection and response**: **Чтение**, **Запись** • **Плейбуки и действия по реагированию**: **Чтение**, **Запись**, **Удаление** • **IAM**: **Чтение пользователей и ролей**, **Назначение ролей** и **Списки пользователей** • **Тенанты**: **Чтение**, **Запись** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**, **Запись** • **Интеграция с приложениями сторонних производителей**: **Чтение**, **Запись** • **Лицензии**: **Чтение** • **Управление активами**: **Чтение**, **Запись**, **Удаление**

Роль	Описание
Младший аналитик	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение** и **Запись** • **Detection and response**: **Чтение** • **Управление активами**: **Чтение** **Просмотр сведений** Чтение: • Просмотр списка категорий. • Просмотр списка устройств в контексте категорий. • Экспорт списка устройств в формат CSV. • Просмотр устройств, удовлетворяющих условиям активной категоризации. • Просмотр карточки актива. • Просмотр списка пользовательских полей. • Просмотр TTL для архивных устройств. • Просмотр параметров аудита активов. • Просмотр параметров интеграции с Open Single Management Platform. • Просмотр пороговых значений для определения статуса активности устройств. Запись: • Добавление категорий. • Изменение категорий. • Добавление устройств. • Изменение устройств, включая категории. • Запуск принудительной синхронизации устройств Open Single Management Platform. • Запуск активной категоризации вручную. • Добавление пользовательских полей актива. • Изменение пользовательских полей актива. • Изменение TTL для архивных устройств. • Добавление параметров аудита активов. • Изменение параметров аудита активов. • Дублирование параметров аудита активов. • Добавление параметров интеграции с Open Single Management Platform. • Изменение параметров интеграции с Open Single Management Platform. • Изменение пороговых значений для определения статуса активности устройств. Удаление: • Удаление категорий. • Архивирование устройств. • Удаление пользовательских полей активов. • Удаление параметров аудита активов. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей** • **Тенанты**: **Чтение** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение** • **Интеграция с приложениями сторонних производителей**: **Чтение** • **Лицензии**: **Чтение**

Роль	Описание
Аналитик 2-го уровня	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение** и **Запись** • **Detection and response**: **Чтение** • **Плейбуки и действия по реагированию**: **Чтение**, **Запись** и **Выполнение** • **Управление активами** • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей** • **Тенанты**: **Чтение** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение** • **Интеграция с приложениями сторонних производителей**: **Чтение** • **Лицензии**: **Чтение**
Аналитик 1-го уровня	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**, **Запись** и **Выполнение**. • **Управление активами.** • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**. Эта роль соответствует роли Аналитик 2-го уровня, но она имеет ограничение. В KUMA аналитик 1-го уровня может изменять только свои собственные объекты.

Роль	Описание
Менеджер SOC	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. **Просмотр сведений** Чтение: • Просмотр списка категорий. • Просмотр списка устройств в контексте категорий. • Экспорт списка устройств в формат CSV. • Просмотр устройств, удовлетворяющих условиям активной категоризации. • Просмотр карточки актива. • Просмотр списка пользовательских полей. • Просмотр TTL для архивных устройств. • Просмотр параметров аудита активов. • Просмотр параметров интеграции с Open Single Management Platform. • Просмотр пороговых значений для определения статуса активности устройств. Запись: • Добавление категорий. • Изменение категорий. • Добавление устройств. • Изменение устройств, включая категории. • Запуск принудительной синхронизации устройств Open Single Management Platform. • Запуск активной категоризации вручную. • Добавление пользовательских полей актива. • Изменение пользовательских полей актива. • Изменение TTL для архивных устройств. • Добавление параметров аудита активов. • Изменение параметров аудита активов. • Дублирование параметров аудита активов. • Добавление параметров интеграции с Open Single Management Platform. • Изменение параметров интеграции с Open Single Management Platform. • Изменение пороговых значений для определения статуса активности устройств. Удаление: • Удаление категорий. • Архивирование устройств. • Удаление пользовательских полей активов. • Удаление параметров аудита активов. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.

Роль	Описание
Подтверждающий	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение, Запись, Закрытие**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение** и **Подтверждение действий по реагированию**. • **Управление активами**: **Чтение**. **Просмотр сведений** Чтение: • Просмотр списка категорий. • Просмотр списка устройств в контексте категорий. • Экспорт списка устройств в формат CSV. • Просмотр устройств, удовлетворяющих условиям активной категоризации. • Просмотр карточки актива. • Просмотр списка пользовательских полей. • Просмотр TTL для архивных устройств. • Просмотр параметров аудита активов. • Просмотр параметров интеграции с Open Single Management Platform. • Просмотр пороговых значений для определения статуса активности устройств. Запись: • Добавление категорий. • Изменение категорий. • Добавление устройств. • Изменение устройств, включая категории. • Запуск принудительной синхронизации устройств Open Single Management Platform. • Запуск активной категоризации вручную. • Добавление пользовательских полей актива. • Изменение пользовательских полей актива. • Изменение TTL для архивных устройств. • Добавление параметров аудита активов. • Изменение параметров аудита активов. • Дублирование параметров аудита активов. • Добавление параметров интеграции с Open Single Management Platform. • Изменение параметров интеграции с Open Single Management Platform. • Изменение пороговых значений для определения статуса активности устройств. Удаление: • Удаление категорий. • Архивирование устройств. • Удаление пользовательских полей активов. • Удаление параметров аудита активов. • **IAM**: **Чтение пользователей и ролей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.

Роль	Описание
Аудитор	Предоставляет следующие права в функциональных областях EDR: • **Алерты и инциденты**: **Чтение**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. **Просмотр сведений** Чтение: • Просмотр списка категорий. • Просмотр списка устройств в контексте категорий. • Экспорт списка устройств в формат CSV. • Просмотр устройств, удовлетворяющих условиям активной категоризации. • Просмотр карточки актива. • Просмотр списка пользовательских полей. • Просмотр TTL для архивных устройств. • Просмотр параметров аудита активов. • Просмотр параметров интеграции с Open Single Management Platform. • Просмотр пороговых значений для определения статуса активности устройств. Запись: • Добавление категорий. • Изменение категорий. • Добавление устройств. • Изменение устройств, включая категории. • Запуск принудительной синхронизации устройств Open Single Management Platform. • Запуск активной категоризации вручную. • Добавление пользовательских полей актива. • Изменение пользовательских полей актива. • Изменение TTL для архивных устройств. • Добавление параметров аудита активов. • Изменение параметров аудита активов. • Дублирование параметров аудита активов. • Добавление параметров интеграции с Open Single Management Platform. • Изменение параметров интеграции с Open Single Management Platform. • Изменение пороговых значений для определения статуса активности устройств. Удаление: • Удаление категорий. • Архивирование устройств. • Удаление пользовательских полей активов. • Удаление параметров аудита активов. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.

Роль	Описание
Взаимодействие с дочерними инцидентами	Предоставляет следующие права в функциональных областях EDR: • **Дочерние инциденты**: **Чтение** и **Запись**. • **IAM**: **Чтение пользователей и ролей**. В дополнение к этой роли у пользователя должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий, Аудитор.
Редактирование общих ресурсов	Предоставляет право изменять доступ к общим ресурсам, расположенным в общем тенанте. В дополнение к этой роли у пользователя должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Чтение общих ресурсов	Предоставляет право на чтение общих ресурсов, расположенных в общем тенанте. В дополнение к этой роли у пользователя должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Управление SLA	Предоставляет право изменять оставшееся время SLA для инцидентов. В дополнение к этой роли у пользователя должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Просмотр универсального макета панели мониторинга	Предоставляет права доступа к просмотру универсального макета панели мониторинга. В дополнение к этой роли у пользователя должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Роли служб	
Автоматическое реагирование на угрозы	Предоставляет учетным записям служб право реагировать на угрозы. Права доступа настраиваются автоматически в соответствии с правами доступа на основе ролей политик Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Вы можете назначать эту роль только учетным записям служб. Эту роль невозможно изменить.

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера, вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Приложение позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи

- Отчеты
- Выборки устройств
- Выборки событий

Чтобы назначить права доступа к конкретному объекту:

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
   - **Управление активами** → **Иерархия групп**.
   - **Задачи**.
   - **Мониторинг** → **Отчеты**.
   - **Управление активами** → **Выборки устройств**.
   - **Мониторинг** → **Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.
4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.
5. Настройте права доступа:
   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
   - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
     - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
     - Если вы хотите назначить пользовательскую роль пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.
6. Нажмите на кнопку **Сохранить**.

Права доступа к объекту настроены.

Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам безопасности, чтобы использовать различные возможности Сервера администрирования и приложений "Лаборатории Касперского", для которых у вас есть плагины управления, например Kaspersky Endpoint Security для Windows.

Чтобы назначить права пользователю или группе безопасности:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

      Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **OK**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
  - Управление группами администрирования
  - Доступ к объектам независимо от их списков ACL
  - Базовая функциональность
  - Удаленные объекты
  - Управление ключами шифрования
  - Обработка событий
  - Операции с Сервером администрирования

    - Теги устройств
    - Развертывание приложений "Лаборатории Касперского"
    - Управление лицензионными ключами
    - Управление отчетами
    - Иерархия Серверов
    - Права пользователей
    - Виртуальные Серверы администрирования
- Управление мобильными устройствами:
    - Общие
- Управление системой:
    - Подключения
    - Инвентаризация оборудования
    - Управление доступом в сеть
    - Развертывание операционной системы
    - Управление уязвимостями и патчами
    - Удаленная установка
    - Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности в область пользовательской роли, чтобы использовать различные возможности Сервера администрирования. Параметры, связанные с ролью пользователя, применяются к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Добавление учетной записи внутреннего пользователя

Чтобы добавить новую учетную запись пользователя Kaspersky EDR Expert:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:

   - **Имя**.

   - **Пароль** для подключения пользователя к Kaspersky EDR Expert.

     Пароль должен соответствовать следующим правилам:

     - Длина пароля должна быть от 10 до 256 символов.

     - Пароль должен содержать символы как минимум трех групп из списка ниже:

       - верхний регистр (A–Z);

       - нижний регистр (a–z);

       - числа (0–9);

       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

     Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

     Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 3. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля".

     Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

5. При необходимости назначьте роли созданной внутренней учетной записи пользователя в тенанте.

Учетная запись пользователей добавлена в список пользователей.

Чтобы войти в систему с помощью созданной учетной записи внутреннего пользователя на консоли OSMP, требуется назначить роль для этой учетной записи. Перед входом удостоверьтесь, что у учетной записи внутреннего пользователя есть роль. В противном случае произойдет ошибка входа в систему.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.

2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:

   - **Имя группы**

   - **Описание**

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп.

Изменение учетной записи внутреннего пользователя

Чтобы изменить учетную запись внутреннего пользователя Kaspersky EDR Expert:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Выберите учетную запись пользователя, которую требуется изменить.

3. В открывшемся окне на вкладке **Общие** измените параметры учетной записи пользователя:

   - **Описание**

   - **Полное имя**

   - **Адрес электронной почты**

- **Основной телефон**
- **Задать новый пароль** для подключения пользователя к Kaspersky EDR Expert.

  Пароль должен соответствовать следующим правилам:

  - Длина пароля должна быть от 10 до 256 символов.
  - Пароль должен содержать символы как минимум трех групп из списка ниже:
    - верхний регистр (A–Z);
    - нижний регистр (a–z);
    - числа (0–9);
    - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  > Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 3. Вы можете изменить разрешенное количество попыток; однако из соображений безопасности не рекомендуется уменьшать это число. Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости переведите переключатель в положение **Выключено**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.

4. На вкладке **Двухфакторная аутентификация** вы можете указать параметры безопасности для этой учетной записи.
5. На вкладке **Группы** можно добавить пользователя или группу безопасности.
6. На вкладке **Устройства** можно назначить устройства пользователю.
7. На вкладке **Роли** можно назначить роль пользователю.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей.

Настройка доменной аутентификации Kerberos

Kaspersky EDR Expert позволяет использовать доменную аутентификацию по протоколу Kerberos. Доменная аутентификация позволяет вам включить безопасную аутентификацию в Консоли OSMP без повторного ввода пароля в корпоративной сети (единый вход).

Сначала вам нужно настроить контроллер домена для использования Kerberos и создать файл keytab. Подробнее см. документацию к контроллеру домена.

SCRIL (для интерактивного входа требуется смарт-карта) поддерживается для Microsoft Active Directory.

Создание файла keytab для FreeIPA и AldPro

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для доступа к контроллеру домена.

2. Если Сервер администрирования находится за пределами домена FreeIPA/AldPro, добавьте запись DNS и запись устройства:

```
ipa dnsrecord-add <zoneName> <recordName> --a-rec <Administration Server IP address>
ipa host-add --password=<password> <Administration Server host address>
```

3. Укажите тип PAC при создании HTTP-сервиса для Сервера администрирования:

```
ipa service-add HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL LETTERS> --ok-to-auth-as-
delegate=true --pac-type PAD
```

   Здесь `<console_host>` – это имя устройства службы, а `<smp_domain>` – это доменное имя. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.

4. Укажите учетную запись для аутентификации:

```
ipa service-allow-retrieve-keytab HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN CAPITAL LETTERS>
--user=<user>
```

5. Экспортируйте файл keytab:

```
ipa-getkeytab -s <domain controller address> -p HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN
CAPITAL LETTERS> -k /tmp/h.keytab
```

Создание файла keytab для Microsoft Active Directory

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для связи с контроллером домена.

2. Включите следующие параметры для учетной записи:

   - **Запрет изменения пароля пользователем.**

   - **Kerberos AES 256-разрядное шифрование.**

   Вы можете включить параметр **Срок действия пароля не ограничен**, чтобы избежать повторной выдачи файла keytab каждый раз, когда истекает срок действия пароля.

3. Добавьте имя субъекта-службы (SPN) в учетную запись:

   ```
   setspn -S HTTP/<> <DOMAIN WRITTEN IN CAPITAL LETTERS>\<user>
   ```

4. Экспортируйте файл keytab:

   ```
   ktpass -out C:\<folder>\<keytab file name> -princ HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL
   LETTERS> -mapuser <user>@<DOMAIN WRITTEN IN CAPITAL LETTERS> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
   <user password> -mapop set
   ```

   Здесь `<console_host>` – это имя устройства службы, а `<smp_domain>` – это доменное имя. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.

Создание файла keytab для Samba

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для связи с контроллером домена:

   ```
   samba-tool user add <user>
   ```

2. Добавьте имя субъекта-службы к учетной записи:

   ```
   samba-tool spn add HTTP/<console_host>.<smp_domain> <user>
   ```

   Здесь `<console_host>` – это имя устройства службы, а `<smp_domain>` – это доменное имя. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.

3. Экспортируйте файл keytab:

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<console_host>.<smp_domain>
```

Включение доменной аутентификации Kerberos

Чтобы включить доменную аутентификацию Kerberos:

1. Выполните опрос контроллеров домена.
2. В главном окне приложения перейдите в раздел **Параметры** → **Единый вход**.
3. Включите параметр **Аутентификация Kerberos**.
4. Загрузите файл keytab.
5. Назначьте доменным пользователям роль, которая предоставляет доступ к Консоли OSMP.

   Доменная аутентификация Kerberos включена для доменных пользователей.

Изменение статуса пользователя

Статус пользователя показывает, можете ли вы назначать пользователю алерты и инциденты.

Пользователи могут иметь один из следующих статусов:

- **Доступен** – пользователь готов работать с алертами и инцидентами.
- **Занят** – пользователь не готов работать с алертами и инцидентами. Алерты и инциденты не могут быть автоматически назначены пользователю.

По умолчанию, когда пользователь входит в Консоль OSMP или Консоль KUMA, статус пользователя автоматически меняется на **Доступен**.

Вы можете вручную изменить статус ваш статус или статус вошедших пользователей.

Изменение статуса вашей учетной записи

Ваш текущий статус отображается в главном окне приложения рядом с именем вашей учетной записи в виде зеленой точки (), если статус **Доступен**, или в виде красной точки (), если статус **Занят**.

Если вы хотите изменить ваш текущий статус, в верхней панели перейдите в параметры своей учетной записи и выберите статус, который будет назначен вашей учетной записи.

Изменение статуса учетной записи внутреннего пользователя

Поле **Статус** в окне параметров учетной записи пользователя, только если пользователь в данный момент вошел в Консоль OSMP или в Консоль KUMA.
Чтобы изменить статус внутреннего пользователя, у вас должна быть одна из следующих EDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC.

Чтобы изменить статус внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей.

2. Нажмите на имя учетной записи пользователя, для которого вы хотите изменить статус.

   Откроется окно параметров учетной записи на вкладке **Общие**.

3. В поле **Статус** выберите статус, который вы хотите назначить: **Доступен** или **Занят**.

4. Нажмите на кнопку **Сохранить**.

Статус пользователя будет изменен.

Изменение группы безопасности

Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.

2. Выберите группу безопасности, которую требуется изменить.

3. В открывшемся окне измените параметры группы безопасности:

   - На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.

   - На вкладке **Пользователи** можно выполнить следующие действия:

     - Просмотреть таблицу пользователей группы.

     - Добавить пользователей в группу безопасности. Для этого нажмите на кнопку **Добавить**, затем в открывшейся панели **Добавить пользователей** установите флажки рядом с учетными записями пользователей, которые вы хотите добавить, и нажмите **Сохранить**.

       В панели **Добавить пользователей** вы можете фильтровать пользователей по тенанту. Для этого укажите необходимое значение критериев фильтра **Тенант-владелец**.

Добавление пользователей в группу безопасности доступно только для внутренних пользователей и для внутренних групп безопасности.

- Удалить пользователей из группы безопасности. Для этого установите флажок рядом с именем учетной записи пользователя, нажмите **Удалить** и подтвердите действие.

- На вкладке **Роли** можно назначить роль группе безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.

   Можно выбрать несколько имен.

3. В меню нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли.

4. Следуйте инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, а затем выберите область применения роли.

   Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

Чтобы добавить учетные записи пользователей в группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.

3. Нажмите на кнопку **Назначить группу**.

4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.

5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Secure Mobility Management.

Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:

   a. В главном меню нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.

3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.

4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.

5. Нажмите на кнопку **Добавить**.

6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.

7. Нажмите на кнопку **OK**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Управление активами** → **Активы (Устройства)**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Настройка двухфакторной аутентификации

Двухфакторная аутентификация включена автоматически, начиная с Kaspersky EDR Expert 2.0. Глобальный параметр выключения двухфакторной аутентификации не поддерживается. Этот сценарий содержит шаги по настройке двухфакторной аутентификации при первом входе в систему и настройке параметров двухфакторной аутентификации на Сервере администрирования.

Этапы

Настройка двухфакторной аутентификации состоит из следующих этапов:

1. **Установка приложения для аутентификации на устройство**

   Вы можете установить любое приложение для аутентификации, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), например:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Рутокен OTP

   Чтобы проверить, поддерживает ли Kaspersky EDR Expert приложение для аутентификации, которое вы хотите использовать, включите двухфакторную аутентификацию для всех пользователей или для определенного пользователя.

   Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky EDR Expert поддерживает выбранное приложение для аутентификации.

   > Категорически не рекомендуется устанавливать приложение для аутентификации на то же устройство, с которого управляется Сервер администрирования.

2. **Синхронизация времени на устройстве с приложением аутентификации со временем устройства, на котором установлен Сервер администрирования**

   Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре. Иначе возможны сбои при настройке двухфакторной аутентификации.

3. **Настройка двухфакторной аутентификации для учетных записей пользователей при входе в Web Console**

   Выполните вход в Web Console и настройте двухфакторную аутентификацию.

   Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и для которого настроена двухфакторная аутентификация, чтобы добавить вашу учетную запись в список допущенных к настройке двухфакторной аутентификации.

4. **Настройка параметров двухфакторной аутентификации на Сервере администрирования**

   Если вы настроили двухфакторную аутентификацию и у вас есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**, вы можете настроить следующие параметры двухфакторной аутентификации на Сервере администрирования:

   1. Просмотр списка пользователей, которые могут настроить двухфакторную аутентификацию при входе в систему:

      - Для чистой установки Kaspersky EDR Expert 2.0: добавьте нужных пользователей в список пользователей с правом настраивать двухфакторную аутентификацию, чтобы они могли настроить двухфакторную аутентификацию при первом входе в систему.

      - Для обновления или восстановления Kaspersky EDR Expert 2.0: просмотрите список пользователей с правом настраивать двухфакторную аутентификацию и удалите учетные записи, которые не должны иметь доступа к Серверу администрирования.

   2. Исключение учетных записей пользователей, для которых не требуется включать двухфакторную аутентификацию (не обязательно).

      Исключите учетные записи пользователей из двухфакторной аутентификации, чтобы разрешить им войти на Сервер администрирования, даже если у них не настроена двухэтапная проверка. Исключение учетных записей из двухэтапной проверки может потребоваться для учетных записей, которые не могут предоставить код безопасности во время аутентификации. Интеграционные учетные записи используются для запуска скриптов с помощью OpenAPI.

   3. Сброс или удаление секретного ключа двухфакторной аутентификации (не обязательно).

      Вы можете сбросить секретный ключ двухфакторной аутентификации, если пользователь теряет доступ к своему устройству двухфакторной аутентификации или ему нужно настроить двухфакторную аутентификацию на новом устройстве. Вы также можете сбросить секретный ключ для своей учетной записи.

      Вы можете удалить секретный ключ, чтобы полностью заблокировать вход пользователя в Web Console и запретить пользователю доступ к Серверу администрирования.

   4. Изменение имени издателя кода безопасности (не обязательно)

      Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

Результаты

После выполнения этого сценария:

- Двухфакторная аутентификация настраивается как для вашей учетной записи, так и для другой учетной записи пользователя, которому требуется доступ к Серверу администрирования.
- Интеграционные учетные записи исключены из двухфакторной аутентификации.

О двухфакторной аутентификации учетной записи

Kaspersky EDR Expert предоставляет пользователям Консоли OSMP возможность использовать двухфакторную аутентификацию. Двухфакторная аутентификация основана на стандарте RFC 6238 (TOTP: Time-Based One-Time Password algorithm – алгоритм временных одноразовых паролей).

При каждом входе в Консоль OSMP пользователь вводит свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Для получения одноразовых кодов безопасности необходимо установить на компьютере или мобильном устройстве приложение для аутентификации.

Может использоваться любое приложение для аутентификации, поддерживающее алгоритм временных одноразовых паролей (TOTP), например, Google Authenticator. Для генерации одноразового кода безопасности системное время, установленное на устройстве с приложением для аутентификации, должно быть синхронизировано со временем, установленным на устройстве с Сервером администрирования. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре.

Для того чтобы проверить, поддерживает ли Kaspersky EDR Expert приложение для аутентификации, которое вы хотите использовать, попробуйте настроить двухфакторную аутентификацию с помощью этого приложения.

На одном из шагов процедуры вводится код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky EDR Expert поддерживает выбранное приложение для аутентификации.

Генерация секретного кода с помощью приложения для аутентификации

Приложение для аутентификации генерирует секретный код следующим образом:

1. Сервер администрирования генерирует специальный секретный ключ и QR-код.
2. Вы передаете сгенерированный секретный ключ или QR-код приложению для аутентификации.
3. Приложение для аутентификации генерирует одноразовый код безопасности, который вы передаете в окно аутентификации Сервера администрирования.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении для аутентификации. Вы можете изменить имя издателя кода безопасности. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. После следующего входа в систему Серверу администрирования будет присвоено новое имя издателя кода безопасности. Код безопасности является одноразовым и действует до 30 секунд (точное время может варьироваться).

Настоятельно рекомендуется сохранить секретный ключ (или QR-код) и хранить его в надежном месте. Этот поможет вам восстановить доступ к Консоли OSMP в случае потери доступа к мобильному устройству.

Следует учитывать следующие особенности двухфакторной аутентификации:

- Начиная с Kaspersky EDR Expert версии 2.0, двухфакторная аутентификация включается автоматически, а возможность настраивать двухфакторную аутентификацию при входе в систему выключена по умолчанию. Настройка двухфакторной аутентификации при входе доступна только пользователям, включенным в список разрешений для настройки двухфакторной аутентификации.

- Пользователь может настроить двухфакторную аутентификацию только для своей учетной записи.

- Пользователь может исключить учетные записи из двухфакторной аутентификации. Это может быть необходимо для интеграционных учетных записей, для которых невозможно получение одноразового кода безопасности для аутентификации. Учетные записи интеграции используются для запуска скриптов через OpenAPI и запуска скриптов KUMA.

- Для генерации нового секретного ключа двухфакторной аутентификации пользователь должен сбросить секретный ключ для своей учетной записи.

- Для сброса или удаления секретного ключа двухфакторной аутентификации других пользователей необходима учетная запись с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

- Для исключения учетных записей пользователей из двухфакторной аутентификации или изменения списка разрешений для настройки аутентификации необходима учетная запись с настроенной двухфакторной аутентификацией и с правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

- Всегда должен быть хотя бы один пользователь с настроенной двухфакторной аутентификацией, чтобы этот пользователь мог управлять списком пользователей с правом настраивать двухфакторную аутентификацию и списком исключений.

- Двухфакторная аутентификация автоматически включается только для Kaspersky EDR Expert версии 2.0. Параметры двухфакторной аутентификации главных или подчиненных Серверов администрирования версии 1.4 или более ранних останутся неизменными.

- Виртуальные Серверы администрирования наследуют параметры двухфакторной аутентификации от соответствующего физического Сервера администрирования, поэтому, если на физическом Сервере администрирования двухфакторная аутентификация включена, она также включается и на виртуальном Сервере администрирования. Настройка параметров двухфакторной аутентификации на виртуальном Сервере администрирования не поддерживается.

Для обеспечения комплексной защиты с помощью двухфакторной аутентификации должна быть обеспечена безопасность не только Сервера администрирования, но и устройства, на котором Сервер установлен. Соответствующие рекомендации приведены в Руководстве по усилению защиты.

Настройка секретного ключа двухфакторной аутентификации при входе в Консоль OSMP

При первом входе в Kaspersky EDR Expert 2.0 или выше откроется окно для настройки двухфакторной аутентификации.

Чтобы настроить двухфакторную аутентификацию для учетной записи:

1. Установите любое приложение, поддерживающее алгоритм временных одноразовых паролей (TOTP), на мобильном устройстве или компьютере, например:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Рутокен OTP

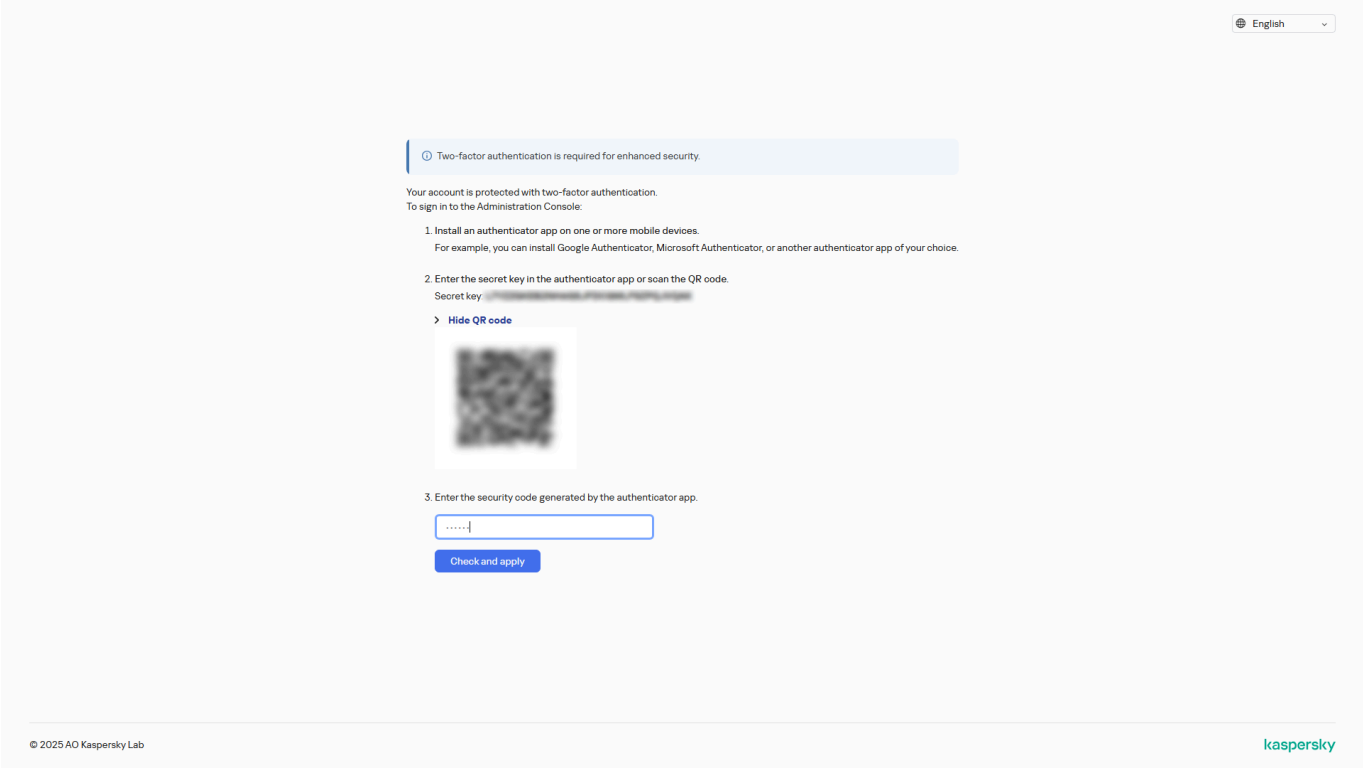
   > Категорически не рекомендуется устанавливать приложение для аутентификации на то же устройство, с которого управляется Сервер администрирования.

2. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре.

3. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве или компьютере. Для этого выполните одно из следующих действий:

   - Вручную введите секретный ключ двухфакторной аутентификации в приложение для аутентификации.
   - Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации.

На мобильном устройстве отобразится одноразовый код безопасности из 6 цифр.



Настройка секретного ключа двухфакторной аутентификации при входе в Консоль OSMP

4. В окне **Двухфакторная аутентификация** укажите код безопасности, сгенерированный приложением для аутентификации, и нажмите на кнопку **Проверить и применить**.

Конфигурация Рутокена OTP

Если вы используете Рутокен OTP, вам потребуется мобильное устройство Android с установленным приложением Рутокен OTP. Мобильное устройство Android должно соответствовать следующим требованиям:

- Операционная система Android 7 или выше.
- NFC-модуль доступен и включен.

В приложении Рутокен OTP необходимо настроить следующие параметры:

- Выполните проверку QR-кода, который отображается в двухэтапном мастере настройки.
- Установите временной интервал – 30 секунд.
- Выберите алгоритм SHA1.

Чтобы настроить Рутокен OTP:

1. Поместите устройство Рутокена OTP рядом с мобильным устройством с NFC-модулем.
2. В приложении Рутокен OTP нажмите **Подключить токен**.
3. В приложении Рутокен OTP нажмите **Настроить параметры**, а затем нажмите **Сохранить секретный ключ**.

Если токен успешно подключен к мобильному устройству, приложение Рутокен OTP отображает следующие сообщения:

- **Токен подключен.**
- **Параметры настроены.**
- **Секретный ключ сохранен.**

4. На устройстве Рутокен OTP нажмите на кнопку.

   На устройстве отобразится код безопасности.

5. В OSMP Console в окне двухфакторной аутентификации введите код безопасности.

Двухфакторная аутентификация для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей** и который настроил двухфакторную аутентификацию, чтобы добавить вашу учетную запись в список пользователей с правом настраивать двухфакторную аутентификацию.

Разрешение для настройки двухфакторной аутентификации пользователям

Список разрешений для настройки двухфакторной аутентификации – это список пользователей, которым разрешена начальная настройка двухфакторной аутентификации при входе в Web Console. В этот список входят учетные записи пользователей, для которых не настроена двухфакторная аутентификация. По умолчанию новые учетные записи не включаются в список разрешений для настройки двухфакторной аутентификации и должны добавляться в этот список администратором. Если новая учетная запись является интеграционной и используется для запуска скриптов OpenAPI, ее необходимо исключить из двухфакторной аутентификации.

Учетная запись пользователя автоматически удаляется из списка, когда для нее настраивается двухфакторная аутентификация или она добавляется в исключения из двухфакторной аутентификации.

Вручную изменять список разрешений для настройки двухфакторной аутентификации разрешено учетным записям с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

Чтобы вручную добавить учетную запись в список разрешений:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств в таблице **Пользователям разрешено генерировать секретные ключи** нажмите на кнопку **Добавить**.

3. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите добавить.

      В список разрешений могут добавляться только пользователи, которые не исключены из двухфакторной аутентификации и не имеют секретного ключа двухфакторной аутентификации.

   b. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   c. Сохраните изменения.

   Выбранная учетная запись пользователя будет добавлена в список разрешений для настройки двухфакторной аутентификации. При следующем входе в систему этому пользователю будет предоставлена возможность сгенерировать секретный ключ.

Удаление учетной записи пользователя из списка разрешений для настройки двухфакторной аутентификации возможно до тех пор, пока для этой учетной записи не будет настроена двухфакторная аутентификация.

Чтобы удалить учетные записи пользователей из списка разрешений для настройки двухфакторной аутентификации вручную:

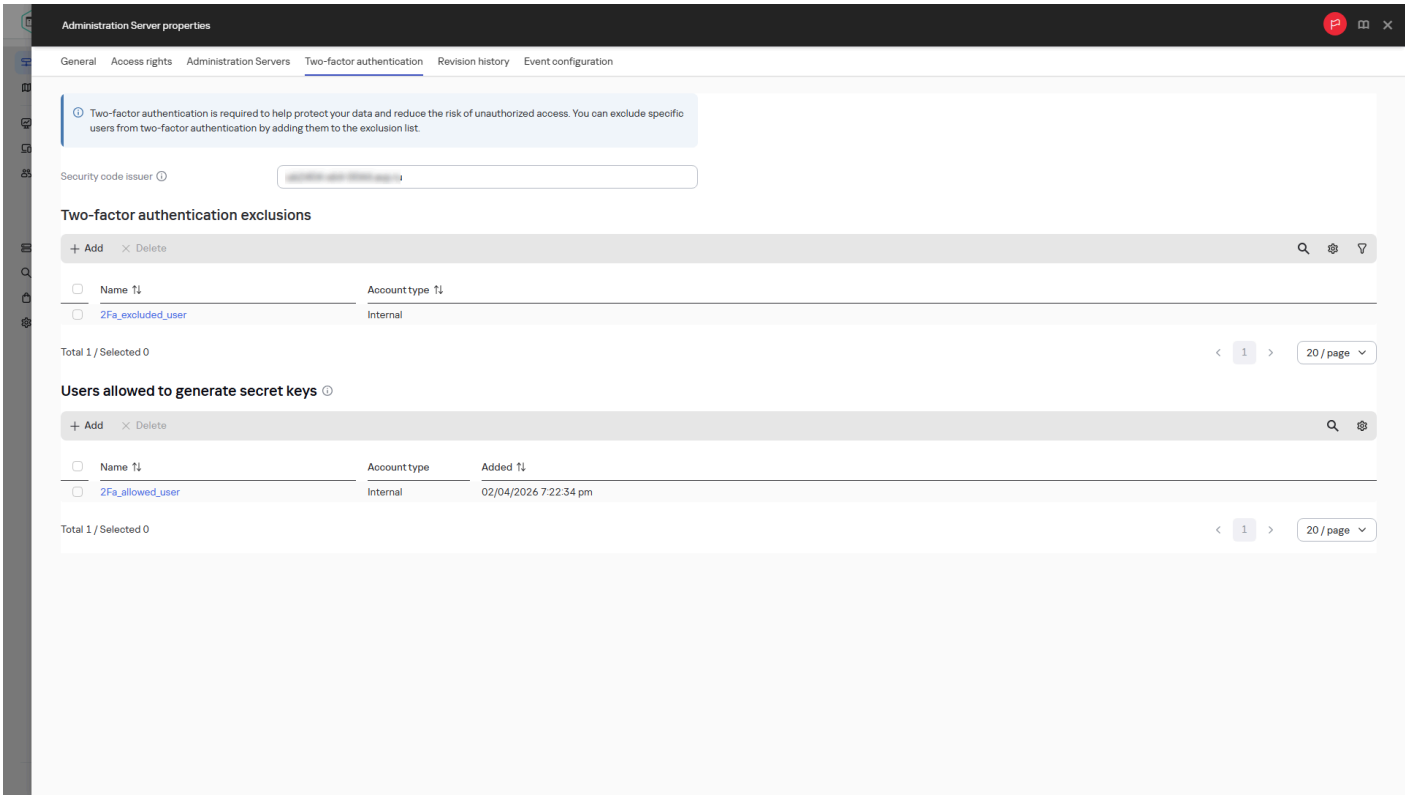
1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств, в таблице **Пользователям разрешено генерировать секретные ключи**, выберите учетные записи, которые требуется удалить, и нажмите на кнопку **Удалить**.

3. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

Выбранные учетные записи пользователей будут удалены из списка разрешений.



Настройка списка разрешений для настройки двухфакторной аутентификации

Если во время активного сеанса на Сервере администрирования ваш секретный ключ двухфакторной аутентификации удален другим пользователем или вы сбросили ключ самостоятельно, не создав нового, возможность вносить изменения в список разрешений будет заблокирована.

Учетные записи пользователей также могут добавляться в список разрешений для настройки двухфакторной аутентификации и удаляться из него автоматически.

При сбросе секретного ключа двухфакторной аутентификации для других учетных записей такие учетные записи автоматически добавляются в список пользователей с правом настраивать двухфакторную аутентификацию, чтобы пользователь мог сгенерировать для себя новый секретный ключ.

При обновлении Kaspersky EDR Expert с версии 1.4 до версии 2.0 или выше учетные записи пользователей будут автоматически добавлены в список разрешений для двухфакторной аутентификации при соблюдении всех следующих условий:

- У пользователя есть право на чтение в функциональной области *Общие функции: Базовая функциональность*, назначенное непосредственно пользователю (не через группу безопасности). Область применения роли пользователя с этим разрешением должна включать все управляемые и нераспределенные устройства и должна быть задана на уровне Сервера администрирования.

- Пользователь не входит в список исключений из двухфакторной аутентификации.

- У пользователя отсутствует секретный ключ двухфакторной аутентификации.
- На Сервере администрирования предыдущей версии двухфакторная аутентификация не была включена для всех пользователей.

Невыполнение хотя бы одного из условий приведет к тому, что пользователь не будет добавлен в список пользователей с правом настраивать двухфакторную аутентификацию.

После обновления или восстановления из резервной копии рекомендуется убедиться, что список разрешений содержит только те учетные записи пользователей, у которых должен быть доступ к Серверу администрирования. Просмотрите список разрешений и удалите из него все лишние учетные записи. Добавьте интеграционные учетные записи, используемые для запуска скриптов через OpenAPI, в список исключений – это необходимо для правильной работы скриптов.

Учетные записи пользователей потеряют доступ к Серверу администрирования после обновления или восстановления, если будут выполнены все следующие условия:

- У пользователя есть право на чтение в функциональной области *Общие функции: Базовая функциональность*, назначенное через группу безопасности (а не непосредственно пользователю), либо вовсе нет этого права.
- Пользователь не входит в список исключений из двухфакторной аутентификации.
- У пользователя отсутствует секретный ключ двухфакторной аутентификации.
- На Сервере администрирования предыдущей версии двухфакторная аутентификация была включена для всех пользователей.

При необходимости эти учетные записи можно добавить вручную в список разрешений для настройки двухфакторной аутентификации.

Сброс и удаление секретного ключа двухфакторной аутентификации

Сброс секретного ключа может потребоваться, если пользователь утратит доступ к своему устройству двухфакторной аутентификации или возникнет необходимость настроить двухфакторную аутентификацию на новом устройстве. Сброс секретного ключа позволяет пользователю войти в Web Console и сгенерировать новый секретный ключ.

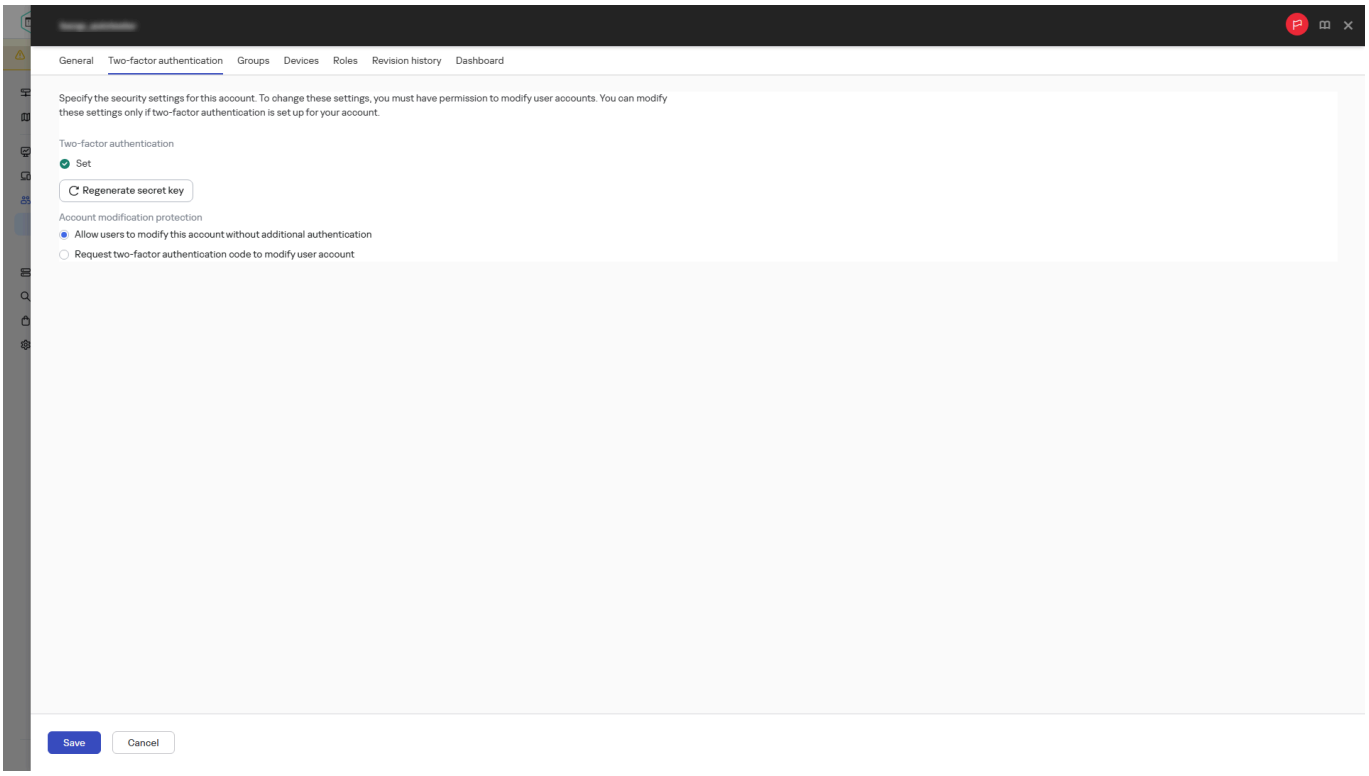
Вы можете сбросить или удалить секретный ключ двухфакторной аутентификации для учетных записей других пользователей, только если у вас настроена двухфакторная аутентификация и есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**. Вы также можете сгенерировать новый секретный ключ для себя.

Чтобы сбросить секретный ключ для учетной записи:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи, для которой нужно сбросить секретный ключ.

3. Если необходимо сбросить секретный ключ для собственной учетной записи:

   a. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Сгенерировать секретный ключ снова**.

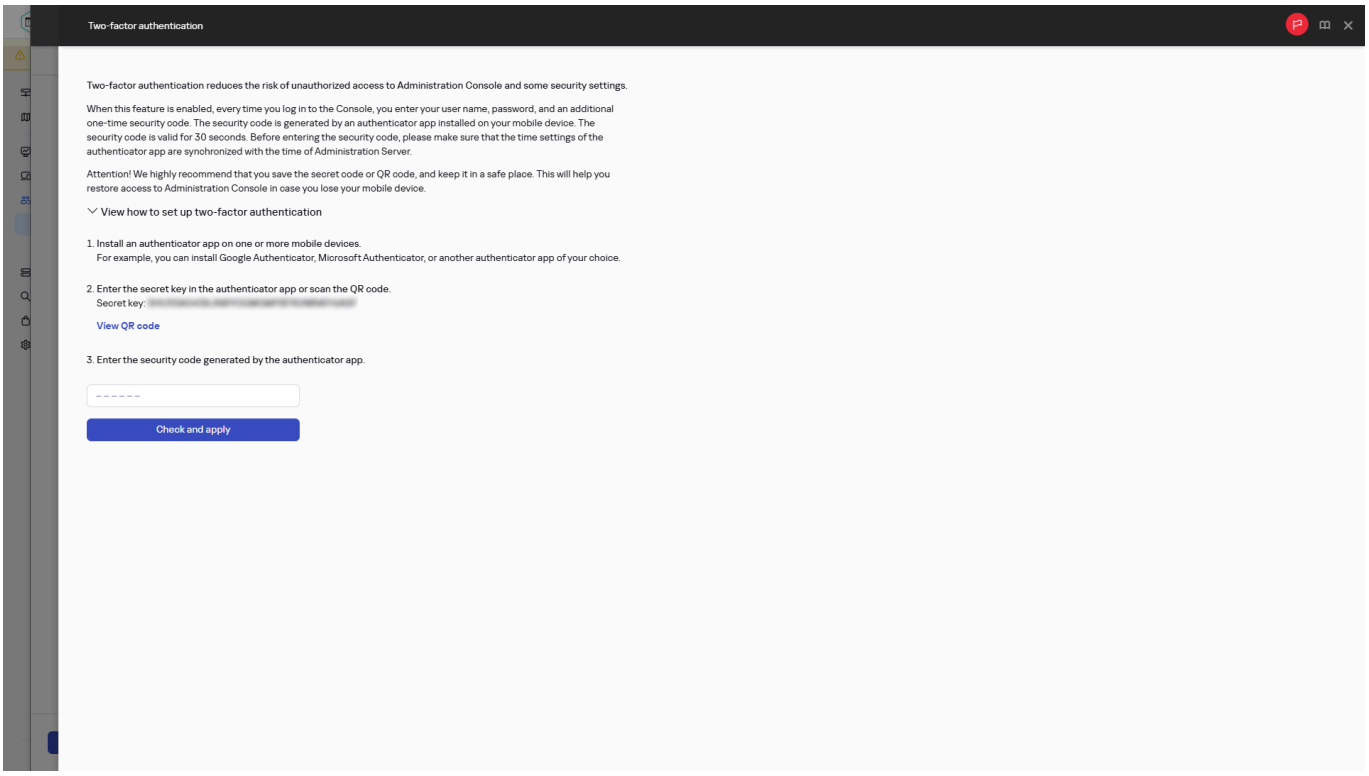


Восстановление секретного ключа двухфакторной аутентификации для текущей учетной записи пользователя

   a. Если ваша учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и код двухфакторной аутентификации.

   b. В окне **Двухфакторная аутентификация** нажмите **Узнайте, как настроить двухфакторную аутентификацию**, затем **Просмотреть QR-код**.

   c. Отсканируйте QR-код в приложении для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.



Настройка нового секретного ключа двухфакторной аутентификации для текущей учетной записи пользователя

a. В окне **Двухфакторная аутентификация** укажите одноразовый код безопасности, сгенерированный приложением для аутентификации, нажмите на кнопку **Проверить и применить**, затем сохраните изменения.

Конфигурация Рутокена OTP

Если вы используете Рутокен OTP, вам потребуется мобильное устройство Android с установленным приложением Рутокен OTP. Мобильное устройство Android должно соответствовать следующим требованиям:

- Операционная система Android 7 или выше.
- NFC-модуль доступен и включен.

В приложении Рутокен OTP необходимо настроить следующие параметры:

- Выполните проверку QR-кода, который отображается в двухэтапном мастере настройки.
- Установите временной интервал – 30 секунд.
- Выберите алгоритм SHA1.

Чтобы настроить Рутокен OTP:

1. Поместите устройство Рутокена OTP рядом с мобильным устройством с NFC-модулем.
2. В приложении Рутокен OTP нажмите **Подключить токен**.
3. В приложении Рутокен OTP нажмите **Настроить параметры**, а затем нажмите **Сохранить секретный ключ**.

Если токен успешно подключен к мобильному устройству, приложение Рутокен OTP отображает следующие сообщения:

- **Токен подключен.**
- **Параметры настроены.**
- **Секретный ключ сохранен.**

4. На устройстве Рутокен OTP нажмите на кнопку.

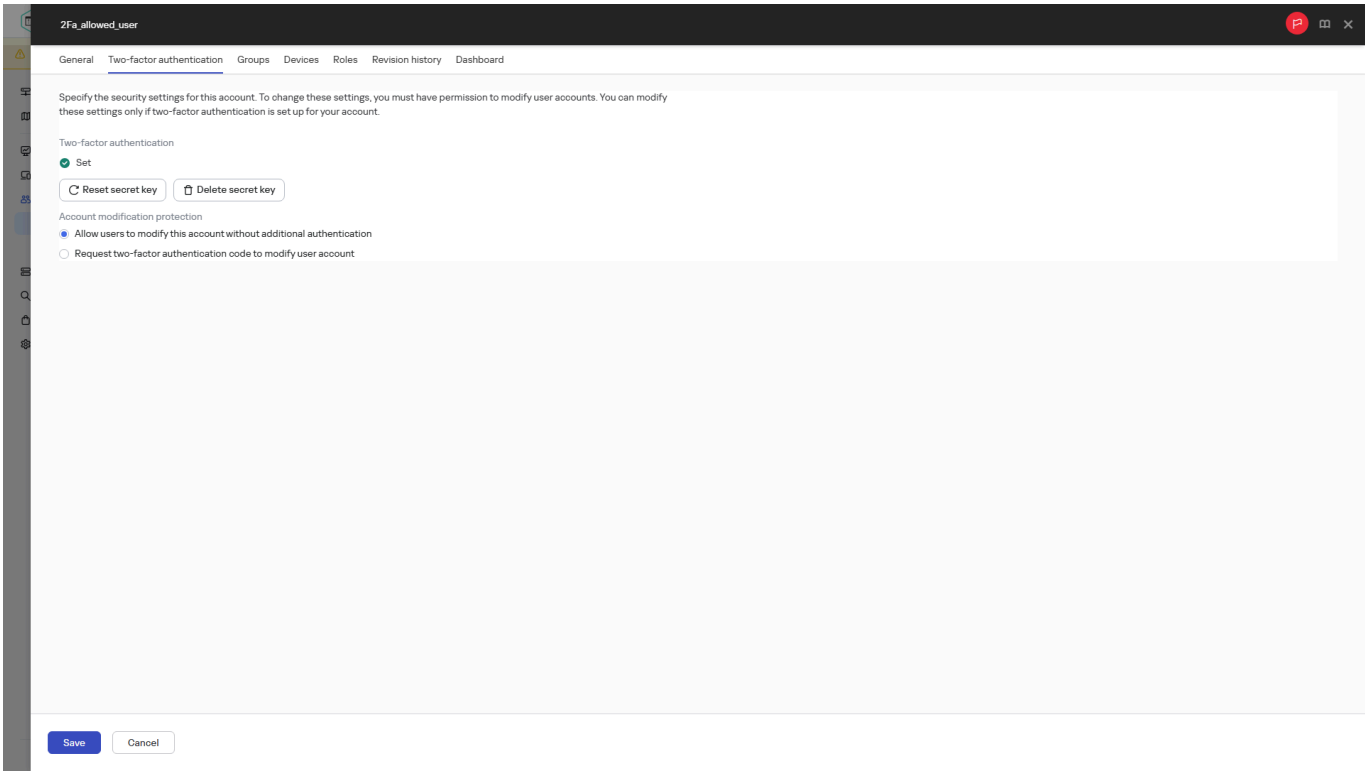
   На устройстве отобразится код безопасности.

5. В OSMP Console в окне двухфакторной аутентификации введите код безопасности.

Секретный ключ вашей собственной учетной записи изменен.

4. Если необходимо сбросить секретный ключ для чужой учетной записи:

   a. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Сбросить секретный ключ**.



Сброс секретного ключа двухфакторной аутентификации для другой учетной записи пользователя

   a. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   b. Подтвердите сброс секретного ключа, а затем сохраните изменения.

При сбросе секретного ключа для другой учетной записи существующий секретный ключ удаляется, а учетная запись добавляется в список разрешений для настройки двухфакторной аутентификации в свойствах Сервера администрирования. При следующем входе в систему пользователь сможет сгенерировать новый секретный ключ.

Секретный ключ учетной записи пользователя будет сброшен.

Вы можете удалить секретный ключ, чтобы полностью заблокировать вход пользователя в Web Console и запретить пользователю доступ к Серверу администрирования.

Чтобы удалить секретный ключ:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Нажмите на имя внутренней учетной записи, для которой требуется удалить секретный ключ.

   Секретный ключ для собственной учетной записи удалить невозможно.

3. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Удалить секретный ключ**.

4. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

5. Подтвердите удаление секретного ключа, а затем сохраните изменения.

Секретный ключ учетной записи пользователя будет удален.

Для восстановления доступа пользователя можно добавить в список разрешений для настройки двухфакторной аутентификации в свойствах Сервера администрирования. В этом случае при следующем входе в систему пользователь сможет сгенерировать новый секретный ключ.

Исключение учетных записей из двухфакторной аутентификации

Учетные записи пользователей можно исключить из двухфакторной аутентификации, чтобы разрешить им входить на Сервер администрирования, даже если у них не настроена двухфакторная аутентификация. Исключение учетных записей из двухфакторной аутентификации может потребоваться для интеграционных учетных записей, которые по техническим причинам не могут предоставлять одноразовый код безопасности во время аутентификации. Учетные записи интеграции используются для запуска скриптов через OpenAPI и запуска скриптов KUMA.

Вносить изменения в список исключений могут учетные записи с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

Чтобы исключить учетную запись пользователя из двухфакторной аутентификации:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** окна свойств в таблице **Исключения двухфакторной аутентификации** нажмите на кнопку **Добавить**.

3. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите исключить.

   b. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   c. Сохраните изменения.

   Выбранные учетные записи пользователей будут исключены из двухфакторной аутентификации, а их секретные ключи (если таковые существуют) будут удалены. Список исключенных учетных записей не изменяется при обновлении Kaspersky EDR Expert до версии 2.0 и выше. Если в предыдущей версии Kaspersky EDR Expert у учетных записей из списка исключений были секретные ключи, в версии 2.0 эти секретные ключи будут удалены.

Удаление учетных записей пользователей из списка исключений полностью запрещает таким пользователям вход в Web Console и не позволяет им осуществлять доступ к Серверу администрирования.

Чтобы удалить учетные записи пользователей из списка исключений:

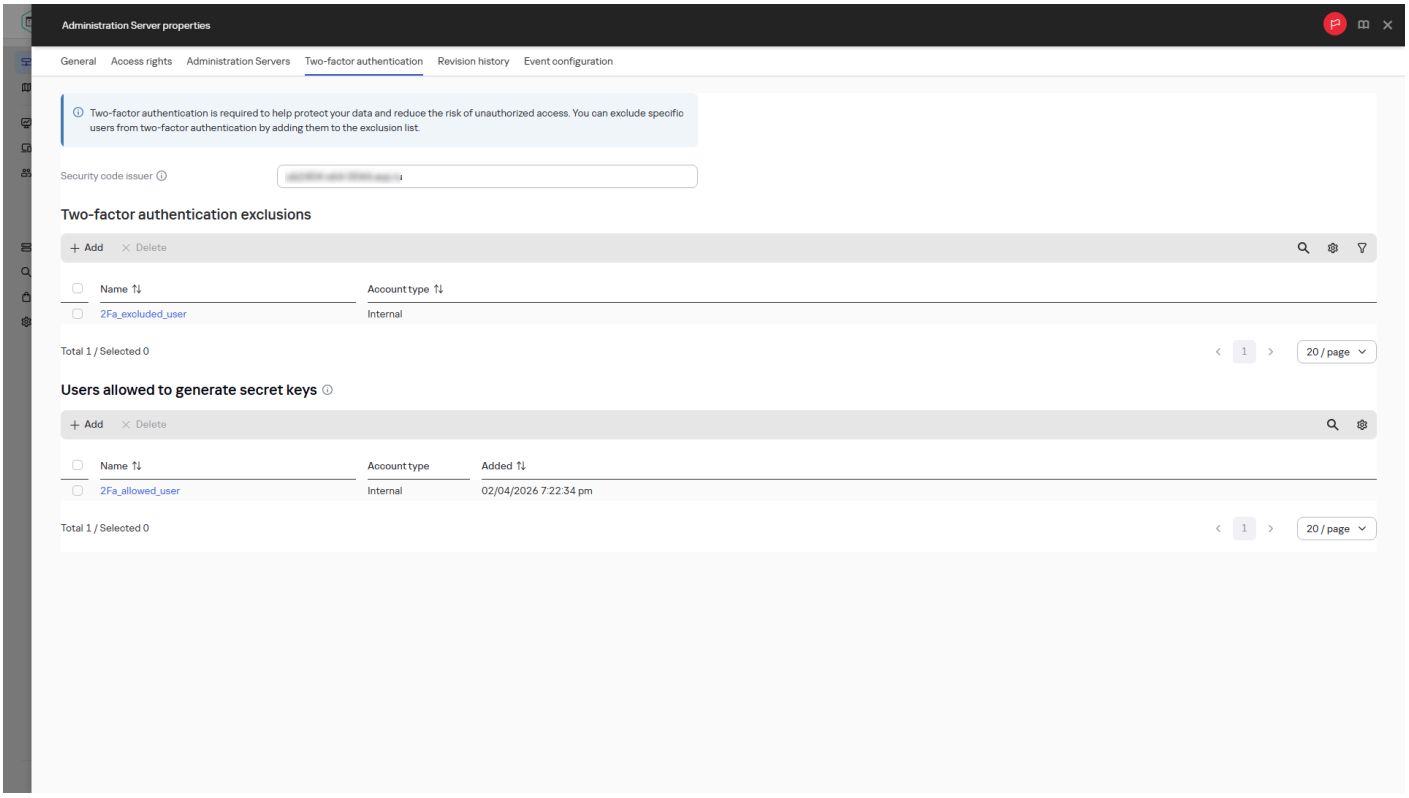
1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. В окне свойств, на вкладке **Двухфакторная аутентификация**, в таблице **Исключения двухфакторной аутентификации**, выберите учетные записи, которые требуется удалить, и нажмите на кнопку **Удалить**.

3. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

Выбранные учетные записи пользователей будут удалены из списка исключений.



Настройка списка исключений двухфакторной аутентификации

Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (далее также издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

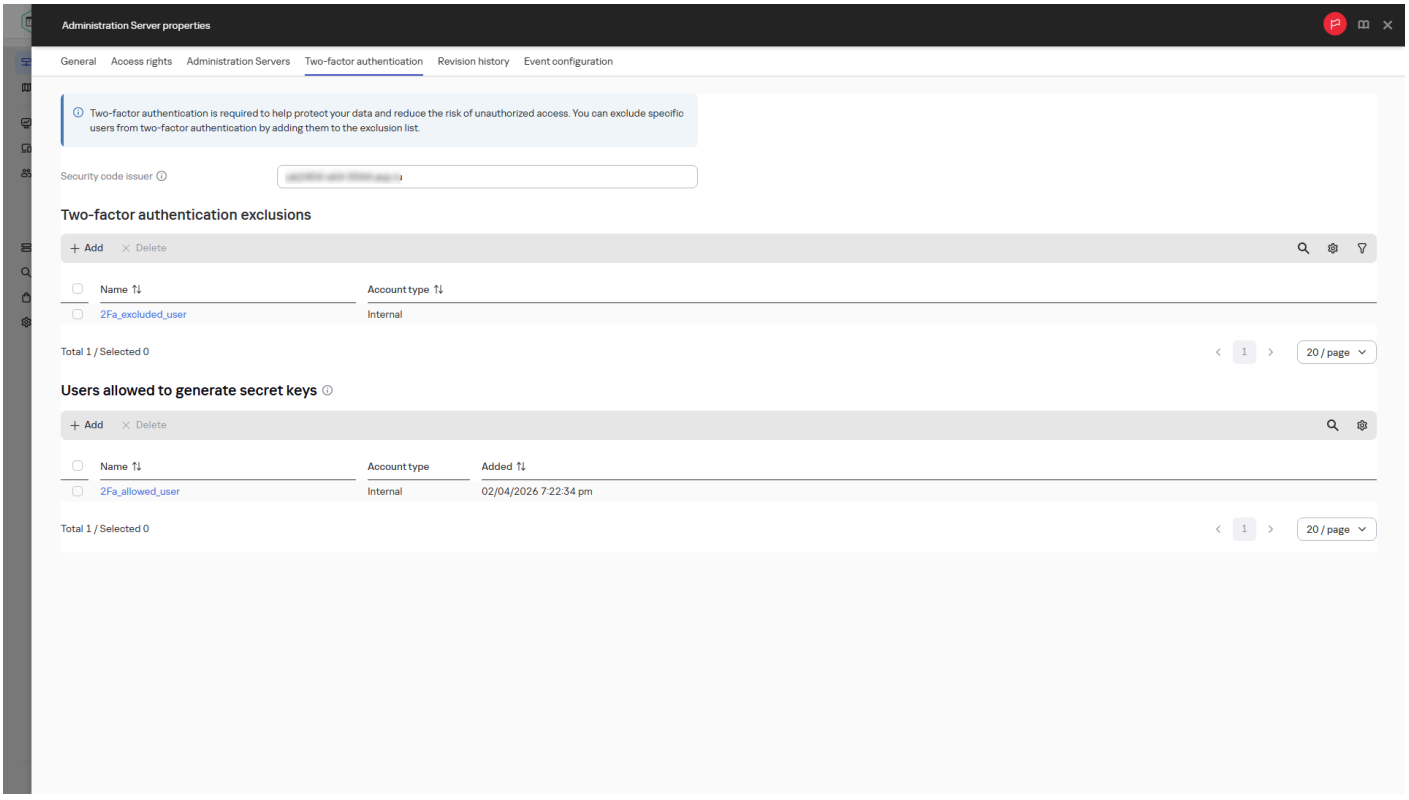
Чтобы указать новое имя издателя кода безопасности:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств введите новое имя в поле **Кем выдан код безопасности**, а затем сохраните изменения.

После следующего входа в систему Серверу администрирования будет присвоено новое имя издателя кода безопасности.



Ввод имени издателя кода безопасности

Количество попыток ввода пароля

Пользователь Kaspersky EDR Expert может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 3. Это количество фиксировано и не может быть изменено.

Настройка времени жизни пользовательских сеансов единого входа и токенов аутентификации

Время жизни токена (или пользовательского сеанса) – это период, в течение которого токен или сеанс остаются действительными и могут использоваться для аутентификации. Когда этот период заканчивается, токен или сеанс автоматически истекает и требуется обновление или повторный вход в систему. Kaspersky EDR Expert позволяет настраивать время жизни токенов доступа, токенов обновления, используемых для обновления токенов доступа, и время жизни сеансов единого входа (SSO) при отсутствии активности пользователя. Указывая более короткое время жизни токена или сеанса единого входа, вы уменьшаете риск несанкционированного доступа в случае компрометации токена.

Вы можете настроить время жизни токенов и сеансов единого входа перед развертыванием Kaspersky EDR Expert на нескольких и на одном узле, указав значения соответствующих параметров (`tokenhub_access_token`, `tokenhub_refresh_token`, `credentials_session_ttl`) в конфигурационном файле. Если значения этих параметров не были указаны во время развертывания, будут использованы значения по умолчанию:

- Для токенов доступа (`tokenhub_access_token`) – 1 час.
- Для токенов обновления (`tokenhub_refresh_token`) – 24 часа.
- Для сеанса единого входа при отсутствии активности пользователя (`credentials_session_ttl`) – 1 час.

Чтобы изменить параметры в уже развернутом решении, используйте команды KDT.

Чтобы проверить текущие значения времени жизни:

На устройстве администратора выполните команду:

```
./kdt invoke iam -a getAuthTTLs
```

Текущие значения времени жизни для токенов доступа, токенов обновления и времени сеанса единого входа отображаются в выходных данных команды как `< часы >h< минуты >m< секунды >s`, например:

- `2h`
- `23h30m`
- `12h55m`

Чтобы настроить время жизни токена доступа:

На устройстве администратора выполните команду:

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=< время_жизни >
```

где `< время_жизни >` – требуемый период в часах, минутах и секундах. Например, `1h` или `1h30m`. Минимальное значение `< время_жизни >` для токена доступа составляет `5m`, а максимальное значение – `2h`.

Чтобы настроить время жизни токена обновления:

На устройстве администратора выполните команду:

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_refresh_token=< время_жизни >
```

где `< время_жизни >` – требуемый период в часах, минутах и секундах. Например, `24h` или `720h30m`. Минимальное значение `< время_жизни >` для токена обновления составляет `12m`, а максимальное значение – `4320h`.

Чтобы настроить время жизни сеанса единого входа при отсутствии активности пользователя:

На устройстве администратора выполните команду:

```
./kdt invoke iam -a setAuthTTLs --param credentials_session_ttl=< время_жизни >
```

где `< время_жизни >` – требуемый период в часах, минутах и секундах. Например, `2h` или `1h30m`. Минимальное значение `< время_жизни >` для простоя сеанса единого входа составляет `5m`, а максимальное значение – `96h`.

Чтобы настроить время жизни сразу для всех параметров:

На устройстве администратора выполните команду:

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=< время_жизни > --param
tokenhub_refresh_token=< время_жизни > --param credentials_session_ttl=< время_жизни >
```

где `< время_жизни >` – требуемый период в часах, минутах и секундах.

Настроено время жизни для токенов аутентификации и сеансов единого входа. Если вы вводите значение за пределами минимального и максимального ограничения, такое значение заменяется значением по умолчанию.

Новое настроенное время жизни применяется только к токенам и сеансам, созданным после сохранения изменений. Срок действия активных токенов и сеансов истекает в зависимости от значений параметров времени жизни, которые действовали на момент их выпуска.

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

Удаление пользователей или групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.

   Всегда должен быть хотя бы один пользователь с настроенной двухфакторной аутентификацией, чтобы этот пользователь мог управлять списком пользователей с правом настраивать двухфакторную аутентификацию и списком исключений.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**.

Пользователь или группа безопасности удалены.

Изменение пароля учетной записи пользователя

Вам может потребоваться изменить пароль учетной записи пользователя, если срок действия текущего пароля истекает или если вы хотите сменить его на более надежный.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 10 до 256 символов.
- Пароль должен содержать символы из групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ~ " ( ) < > ;).
- Пароль не должен содержать пробелов и символов в кодировке Unicode.

Изменение пароля учетной записи внутреннего пользователя

Чтобы изменить пароль учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Выберите учетную запись пользователя, которую требуется изменить.

3. В открывшемся окне свойств пользователя на вкладке **Общие** нажмите на кнопку **Изменение пароля**.

4. Установите новый пароль для подключения пользователя к Open Single Management Platform.

   Чтобы посмотреть введенный пароль, нажмите на кнопку 👁.

5. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

6. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

Принудительная смена пароля при первом входе в систему

Вы можете запросить смену паролей при первом входе пользователей в Консоль Open Single Management Platform. Рекомендуется использовать этот параметр, если для нескольких новых учетных записей был выбран один временный пароль, – данный параметр гарантирует, что каждый пользователь укажет собственный пароль при первом входе в систему.

Чтобы принудительно изменить пароль при первом входе в систему:

1. В главном меню приложения перейдите в **Параметры** → **Политики аутентификации** и включите параметр **Принудительно сменить пароль при первом входе**.

2. Сохраните изменения.

Принудительная смена пароля при первом входе включена.

Принудительное изменение пароля определяется во время создания учетной записи пользователя и не применяется ретроспективно:

- Учетные записи, созданные с включенным этим параметром, всегда требуют смены пароля после первого входа в систему, даже если этот параметр был выключен позже.

- Учетные записи, созданные с выключенным параметром, не требуют смены пароля после первого входа в систему, даже если этот параметр был включен позже.

Настройка срока действия пароля

Вы можете настроить срок действия пароля для учетных записей пользователей, чтобы обеспечить более частую смену пароля. По умолчанию параметр включен.

Чтобы изменить срок действия пароля:

1. В главном меню приложения перейдите в **Параметры** → **Политики аутентификации** и включите параметр **Требовать регулярную смену пароля**.

2. В поле **Время действия пароля (сут)** укажите период, по истечении которого срок действия пароля истечет. По умолчанию срок действия пароля 365 дней.

3. Сохраните изменения.

Срок действия пароля изменен.

Добавление пользовательского баннера на страницу входа

На страницу входа можно добавить пользовательский баннер, демонстрирующий пользователям важную информацию перед авторизацией. Например, пользователям можно информировать о мерах информационной безопасности.

Чтобы добавить пользовательский баннер, выполните следующие действия:

1. **Создайте строку баннера**.

   Чтобы создать строку баннера:

   1. Напишите HTML-код для баннера, например:

      ```
      <div>
        <h4>Защищенная система ООО «Ромашка»</h4>
        <p>К работе с системой допускаются только авторизованные сотрудники.</p>
      </div>
      ```

      Добавление изображений не поддерживается.

      Сохраните этот код в файле, например, markup.html.

   2. Закодируйте HTML-код в Base64. В Linux для кодирования используется следующая команда:

      ```
      base64 -w 0 markup.html > banner.b64
      ```

      Команда вернет закодированную строку, например:

      ```
      PGRpdj4KPGg0PtCX0LDRidC40YnQtdC90L3QsNGPINGB0LjRgdGC0LXQvNCwINCe0J7QniDCq9Cg0L7QvNCw0YjQutCwwrs8aDQ+CjxwPtCaIN
      ```

2. Добавьте строку в конфигурацию Kaspersky EDR Expert. Вы можете добавить строку баннера в конфигурацию разными способами:

   - **Добавление баннера при первоначальной настройке**

     Чтобы добавить баннер во время первоначальной настройки:

     1. Перед запуском установки Kaspersky EDR Expert добавьте следующие строки в раздел `parameters` файла param.yaml:

        ```
        - name: login_markup_b64
            source:
            value: "<ваша строка баннера в кодировке Base64>"
        ```

     2. Запустите установку Kaspersky EDR Expert.

- **Добавление баннера при обновлении**

  Чтобы добавить баннер во время обновления:

  1. На устройстве администратора экспортируйте текущий конфигурационный файл с помощью следующей команды:

     ```
     ./kdt ec -e <имя_конфигурационного_файла_и_путь>
     ```

     Текущая версия конфигурационного файла сохраняется в указанной директории с указанным именем.

  2. В секции `parameters` экспортированного конфигурационного файла добавьте следующие строки:

     ```
     - name: login_markup_b64
         source:
         value: "<ваша строка баннера в кодировке Base64>"
     ```

  3. Обновите Kaspersky EDR Expert и компонент Bootstrap. Если вы запускаете команду обновления, укажите полный путь к экспортированному конфигурационному файлу из шага 1 с помощью флага `-i`:

     ```
     ./kdt apply -k <полный_путь_к_архиву_обновлений_XDR> --force --accept-eula -i
     <имя_конфигурационного_файла_и_путь>
     ```

- **Добавление баннера с помощью командной строки**

  Чтобы добавить баннер с помощью командной строки:

  1. Экспортируйте ConfigMap в файл:

     ```
     kubectl get configmap credentials -n iam -o yaml > credentials.yaml
     ```

     Файл credentials.yaml содержит начальную конфигурацию, которую необходимо изменить.

  2. Вставьте Base64-строку баннера в файл credentials.yaml:

     ```
     sed -i 's|public:\\n|public:\\n      login_markup_b64: \\"'"$(sed 's|[\/&\\]|\\&|g'
     banner.b64)"'\\"\\n|' credentials.yaml
     ```

     Эта команда находит строку, содержащую 'public:\n', и вставляет сразу после нее поле `login_markup_b64`.

  3. Используя любой текстовый редактор, убедитесь, что до и после параметра `login_markup_b64` есть ровно шесть пробелов и что кавычки правильно экранированы. Пример:

     ```
     6 пробелов до login_markup_b64:
     \"PGRpdj4KICA8aDQ+WW91ckNvbXBhbnkgU2VjdXJlIFN5c3RlbTwvaDQ+CiAgPHA+T25seSBhdXRob3JpemVkIGVtcGxveWVlcyBhcmUgY
     6 пробелов после
     ```

  4. Примените локальные изменения к кластеру Kubernetes:

     ```
     kubectl apply -f credentials.yaml
     kubectl -n iam rollout restart deployment credentials
     ```

Если вы хотите изменить или удалить баннер позже:

1. Выполните команду:

```
kubectl edit configmap credentials -n iam
```

2. Измените значение параметра `login_markup_b64` или удалите параметр.

3. Примените локальные изменения к кластеру Kubernetes:

```
kubectl apply -f credentials.yaml
kubectl -n iam rollout restart deployment credentials
```

- **Добавление баннера с помощью IDE Lens**

Чтобы добавить баннер с помощью IDE Lens:

1. Загрузите и установите IDE Lens.

2. Скопируйте содержание файла `~/.kdt/cluster.config`.

3. В IDE Lens перейдите в раздел **Локальные kubeconfig-файлы** → **+** → **Добавить kubeconfig путем вставки** и вставьте содержимое файла `cluster.config`.

4. Откройте добавленное пространство имен (`iam`), перейдите в раздел **Config** → **Config Maps** и найдите `учетные данные` ConfigMap.

5. Откройте `учетные данные` ConfigMap и добавьте в конец следующую строку (без отступов):

```
credentials.server.public.login_markup_b64: "<строка вашего баннера в кодировке Base64>"
```

   Пример:

```
credentials.server.public.login_markup_b64:
"PGRpdiBzdHlsZT0idGV4dC1hbGlnbjogY2VudGVyOyI+CiAgPGltZyBzcmM9ImZpbGU6Ly8vaG9tZS90b29yLzUwLmpwZyIgYWx0PSJTZW
```

6. Нажмите на кнопку **Сохранить**.

7. Перезагрузите под:

```
kubectl -n iam rollout restart deployment credentials
```

Чтобы изменить или удалить баннер позже:

1. Повторите шаги с 1 по 4, указанные выше.

2. Откройте `учетные данные` ConfigMap и измените или удалите параметр `login_markup_b64`.

3. Нажмите на кнопку **Сохранить**.

4. Перезагрузите под:

```
kubectl -n iam rollout restart deployment credentials
```

После применения новой конфигурации пользовательский баннер будет отображаться на странице входа.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **OK**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.

- На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.

- На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:

Способ 1:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажки напротив имен пользователей или групп безопасности, которые требуется добавить в область роли.

3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На шаге **Выбор роли** выберите роль, которую требуется назначить.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 2:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.

3. В открывшемся окне свойств роли выберите вкладку **Параметры**.

4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. На шаге **Выбор пользователей** выберите пользователей и группы безопасности, которые требуется добавить в область роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Нажмите на кнопку **Закрыть** (×), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 3:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым вы хотите добавить область пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, примените и сохраните изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Установите флажок напротив роли, которую требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**.

Роль пользователя будет удалена.

Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования. Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

Чтобы связать роль с профилем политики:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на вкладке **Общие**.
3. Перейдите на вкладку **Параметры** и прокрутите вниз до раздела **Политики**.
4. Нажмите на кнопку **Изменить**.
5. Чтобы связать роль с:
   - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.
   - **Новым профилем политики**:

     a. Установите флажок около политики, для которой вы хотите создать профиль политики.

     b. Нажмите на кнопку **Новый профиль политики**.

     c. Укажите имя нового профиля политики и настройте параметры профиля политики.

     d. Нажмите на кнопку **Сохранить**.

     e. Установите флажок рядом с новым профилем политики.
6. Нажмите на кнопку **Назначить роли**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

Мультитенантность

Kaspersky EDR Expert поддерживает мультитенантный режим. Этот режим позволяет главному администратору предоставлять функциональность Kaspersky EDR Expert нескольким клиентам независимо или разделять активы, параметры приложения и объекты для разных офисов. Каждый клиент или офис изолирован от других и называется тенантом.

Обычно режим мультитенантности используется в следующих случаях:

- Поставщик услуг имеет несколько клиентских организаций и хочет предоставить функциональность Kaspersky EDR Expert каждой клиентской организации в отдельности. Для этого администратор поставщика услуг может создать тенант для каждой клиентской организации.

- Администратор крупного предприятия может захотеть изолировать параметры активов и приложений и объекты для офисов или подразделений организации и управлять офисами или подразделениями организации независимо. Для этого администратор может создать тенант для каждого офиса или подразделения.

Мультитенантный режим имеет следующие особенности:

- Изоляция тенантов.

- Межтенантные сценарии.

Изоляция тенантов.

Тенант изолирован и управляется независимо от других тенантов. Только пользователи, которым назначены права доступа к тенанту, могут работать с этим тенантом и управлять им. Администратор другого тенанта не может получить доступ к данным, ресурсам и активам тенанта, если только главный администратор не предоставит соответствующие права доступа администратору в явном виде.

Для каждого тенанта вы определяете ряд объектов, в том числе следующие:

- Активы

  Список активов уникален для каждого тенанта. Каждый актив может принадлежать только одному тенанту.

- Пользователи и их права доступа.

- События, алерты и инциденты.

- Плейбуки

- Интеграция с другими приложениями и службами "Лаборатории Касперского", а также с решениями сторонних производителей.

Межтенантные сценарии.

Все тенанты организованы в иерархию тенантов. По умолчанию иерархия тенантов содержит предварительно созданный корневой тенант вверху иерархии. Никакие другие тенанты не могут быть созданы на том же уровне, что и корневой тенант. Вы создаете тенант в качестве дочернего по отношению к любому существующему тенанту, включая корневой тенант. Иерархия тенантов может иметь любое количество уровней вложенности.

Иерархия тенантов используется для предоставления кросс-тенантных сценариев, включая следующие:

- Наследование и копирование

  Дочерний тенант получает от родительского тенанта следующие объекты:

  - Пользователи и их права доступа.

    Права доступа наследуются по иерархии и не могут быть отозваны на более низком уровне иерархии.

  - Параметры тенанта, включая параметры интеграции

    Параметры тенанта копируются из родительского тенанта в его дочерний тенант. После создания дочернего тенанта вы можете настроить скопированные параметры в соответствии с требованиями нового тенанта.

  Правила агрегации и сегментации наследуются только на один уровень ниже в иерархии тенантов. Например, правило, созданное в корневом тенанте, наследуется дочерними тенантами первого уровня, но не их дочерними тенантами.

- Лицензирование

  Лицензионный ключ для Kaspersky EDR Expert применяется на уровне главного Сервера администрирования, который привязан к корневому тенанту. Далее лицензионный ключ автоматически применяется ко всем тенантам в иерархии.

Роли пользователей.

Kaspersky EDR Expert предоставляет вам заранее определенный набор ролей пользователей. Вы предоставляете пользователям права на управление тенантами, назначая пользователям роли.

Роли пользователей.	Права пользователей		
	Чтение.	Запись.	Удалить
Главный администратор	✓	✓	✓
Администратор тенанта	✓	✓	✓
Администратор SOC	✓	✓	—
Аналитик 1-го уровня	✓	—	—
Аналитик 2-го уровня	✓	—	—
Младший аналитик	✓	—	—
Менеджер SOC	✓	—	—

Роли пользователей.	Права пользователей		
	Чтение.	Запись.	Удалить
Подтверждающий	✓	—	—
Аудитор	✓	—	—
Взаимодействие с дочерними инцидентами	✓	—	—

Тенанты и Серверы администрирования

Вы можете привязать только физические Серверы администрирования к тенантам. Связь между тенантом и Сервером администрирования позволяет объединить возможности обоих решений – Kaspersky EDR Expert и Open Single Management Platform.

Фильтр тенантов в интерфейсе приложения

В интерфейсе Kaspersky EDR Expert вы можете настроить списки объектов для отображения только тех объектов, которые относятся к выбранным тенантам. Фильтр тенантов применяется к следующим объектам:

- Алерты в разделе **Алерты**.
- Инциденты в разделе **Инциденты**.
- События в разделе **Поиск угроз**.
- Плейбуки в разделе **Плейбуки**.

Когда вы применяете фильтр тенантов, новые параметры применяются ко всем типам объектов в интерфейсе Консоли, которую вы используете (Консоль OSMP или Консоль KUMA).

О привязке Серверов администрирования к тенантам

Вы можете привязать Серверы администрирования к тенантам. Связь между тенантом и Сервером администрирования позволяет связать активы, которыми управляет Сервер администрирования, с тенантом.

Вы не можете привязать к тенантам виртуальные Серверы администрирования, только физические.

У тенантов могут быть субтенанты, поэтому они организованы в иерархию тенантов. Серверы администрирования могут иметь подчиненные Серверы администрирования, поэтому они организованы в иерархию Серверов. Вы не можете привязать произвольный Сервер к произвольному тенанту, поскольку это может привести к недопустимой привязке. Например, пользователь может не иметь прав доступа к тенанту в иерархии тенантов, но тот же пользователь может иметь права доступа к устройствам этого тенанта. Это может произойти, если у этого пользователя есть права доступа к Серверу администрирования 2, который является главным для Сервера администрирования 1, привязанного к тенанту. Следовательно, по умолчанию этот пользователь унаследовал права доступа к Серверу администрирования 1 и его управляемым устройствам. Чтобы исключить такую ситуацию, привязывать тенанты и Серверы администрирования друг к другу можно только в соответствии с правилами привязки.

Есть два типа привязок:

- Явная привязка.

  Этот тип привязки устанавливается при выборе Сервера администрирования, который вы хотите привязать к тенанту.

- Унаследованная привязка.

  Когда вы устанавливаете явную привязку для Сервера администрирования, у которого есть подчиненные Серверы администрирования, подчиненные Серверы администрирования привязываются к тенанту через унаследованный тип привязки. Таким образом, к тенанту могут быть привязаны несколько Серверов администрирования.

Правила привязки:

- Корневой Сервер администрирования всегда привязан к корневому тенанту. Вы не можете удалить эту привязку.

- У тенанта не может быть привязанного Сервера администрирования. У такого тенанта могут быть субтенанты, и к этим субтенантам могут быть привязаны Серверы администрирования.

- Вы можете привязать два Сервера администрирования, которые организованы в иерархию, только к двум тенантам, которые также организованы в иерархию, и только если иерархия Серверов администрирования совпадает с иерархией тенантов.

- Сервер администрирования может быть привязан только к одному тенанту явно или через унаследованный тип привязки.

- При явной привязке Сервера администрирования к тенанту:

  - Если Сервер администрирования был привязан к другому тенанту явно, эта привязка автоматически удаляется.

  - Если у Сервера администрирования есть подчиненные Серверы администрирования, подчиненные Серверы администрирования привязываются к новому тенанту через унаследованный тип привязки, за исключением тех Серверов администрирования, которые были привязаны к своим тенантам явно. Перед этой операцией Kaspersky EDR Expert проверяет, все ли новые привязки законны. В противном случае привязка не может быть установлена.

- При удалении явной привязки между тенантом и Сервером администрирования (отмена привязки Сервера администрирования) Сервер администрирования и все его подчиненные Серверы администрирования (если есть) автоматически привязываются через унаследованный тип привязки к тенанту, к которому привязан главный Сервер администрирования выбранного Сервера администрирования. Если некоторые из подчиненных Серверов администрирования привязаны к своим тенантам явно, эти Серверы администрирования сохраняют свои привязки.

- При добавлении нового Сервера администрирования в иерархию этот Сервер администрирования автоматически привязывается через унаследованный тип привязки к тенанту, к которому привязан его главный Сервер администрирования.

- Когда вы удаляете Сервер администрирования из иерархии и Сервер администрирования имеет явную привязку к тенанту, эта привязка удаляется.

Настройка интеграции с Open Single Management Platform

Вы можете привязать Серверы администрирования к тенантам. Связь между Сервером администрирования и тенантом позволяет связать активы, которыми управляет Сервер администрирования, с тенантом.

Вы не можете привязать к тенантам виртуальные Серверы администрирования, только физические.

Предварительные условия:

- Убедитесь, что вы знакомы с правилами привязки.

- Вы создали тенант, к которому хотите привязать Сервер администрирования.

- При необходимости вы добавили подчиненный Сервер администрирования, который хотите привязать к тенанту.

Чтобы привязать Сервер администрирования к тенанту или удалить его привязку к тенанту, вам требуется роль, которая предоставляет право на **Запись** в функциональных областях Тенанты и Интеграции.

Привязка Сервера администрирования к тенанту

Чтобы привязать Сервер администрирования к тенанту:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** в разделе **Интеграции** выберите **KSC**.

4. Нажмите на кнопку **Привязать Сервер администрирования** и в открывшемся окне выберите Сервер администрирования, который вы хотите привязать к тенанту.

   Если вы хотите добавить новый Сервер в иерархию или удалить существующий, вы можете сделать это в свойствах Сервера администрирования.

5. Нажмите на кнопку **Привязать**.

Процесс привязки может занять некоторое время. Вы можете отслеживать этот процесс в столбце **Статус привязки** списка Серверов администрирования в окне свойств тенанта.

Удаление привязки Сервера администрирования к тенанту

Чтобы удалить привязку Сервера администрирования к тенанту:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** установите флажок рядом с Сервером администрирования, для которого вы хотите удалить привязку к тенанту, а затем нажмите на кнопку **Удалить привязку**.

Просмотр и изменение тенантов

Вы можете использовать тенанты, чтобы предоставлять функциональность Kaspersky EDR Expert клиентской организации независимо или разделять активы и параметры приложения и объекты для разных офисов.

Чтобы просмотреть или изменить свойства тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта. Если у вас есть права доступа только для **Чтения** к этому тенанту, свойства будут открыты в режиме только для чтения. Если у вас есть право на **Запись**, вы сможете изменять свойства тенанта.

3. Измените свойства тенанта и нажмите на кнопку **Сохранить**.

   Вы можете нажать на кнопку **Сохранить и закрыть**, чтобы сохранить изменения и закрыть окно свойств тенанта.

Свойства тенанта изменены и сохранены.

Общие.

Вкладка **Общие** содержит общую информацию о тенанте. Вы можете изменить имя и описание тенанта.

Settings

Вкладка **Параметры** содержит следующие разделы:

- **Интеграции с приложениями "Лаборатории Касперского"**

  В этом разделе вы можете настроить параметры интеграции приложений "Лаборатории Касперского", которые вы хотите интегрировать в Kaspersky EDR Expert для текущего тенанта.

- **Интеграция со сторонними приложениями**

  В этом разделе вы можете настроить параметры интеграции для сторонних приложений, которые вы хотите интегрировать в Kaspersky EDR Expert для текущего тенанта.

- **Обнаружения и реагирование**

  В этом разделе можно настроить параметры и объекты, связанные с обнаружением угроз и реагированием на них:

  - Правила сегментации
  - Правила агрегации
  - Подключение к почтовому серверу
  - Аудит активов
  - Учетные данные для сетевых папок
  - Шаблоны электронных писем
  - Параметры проверки
  - Параметры активов
    - Срок хранения архивных активов
    - Настраиваемые поля активов
    - Импорт активов KSC
    - Импорт активов KICS/KATA
  - Репутационная база KPSN

- Срок хранения

  Сроки хранения алертов и инцидентов зависят от лицензии Kaspersky EDR Expert, которую вы используете.

- Управление инцидентами.

Вам не нужно настраивать параметры общего тенанта.

Роли

На вкладке **Роли** перечислены пользователи, имеющие права доступа к тенанту. Вы можете изменить этот список и назначить пользователям роли.

Добавление тенантов

Прежде чем начать, ознакомьтесь с общей информацией о тенантах.

Чтобы добавлять дочерние тенанты, у вас должны быть права на **Чтение** и **Запись** в функциональной области **Тенанты** в родительском тенанте или в тенанте более высокого уровня в иерархии тенантов.

Чтобы добавить тенант:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Установите флажок рядом с родительским тенантом. Новый тенант будет создан как дочерний по отношению к выбранному тенанту.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Добавить тенант** введите имя нового тенанта.
5. При необходимости добавьте описание тенанту.
6. Нажмите на кнопку **Добавить**.

Новый тенант появится в списке тенантов.

Дочерний тенант наследует от родительского тенанта следующие объекты:

- пользователей и их права доступа;
- параметры интеграции.

После создания тенанта вы можете перенастроить унаследованные объекты в соответствии с требованиями нового тенанта.

Назначение ролей пользователям и группам тенанта

Вы можете назначать EDR-роли пользователям Kaspersky EDR Expert и группам домена, чтобы предоставить им наборы прав доступа в тенанте.

Для этого у вас должна быть одна из следующих EDR-ролей в тенанте, в котором вы хотите назначить роли пользователям: Главный администратор, Администратор SOC или Администратор тенанта.

Так как тенанты изолированы и управляются независимо от других тенантов, только пользователи, которым назначены права доступа к тенанту, могут работать с этим тенантом и управлять им.

Права доступа наследуются по иерархии и не могут быть отозваны на более низком уровне иерархии.

Новые внутренние учетные записи пользователей в Консоли OSMP становятся доступными для добавления и назначения ролей в тенанте в течение пяти минут после создания учетной записи.

Права пользователя представляют собой объединение собственных прав пользователя и прав групп домена, к которым принадлежит пользователь при их наличии. Это справедливо, если пользователь включен в группу напрямую или косвенно, когда он входит во вложенную группу. Например, если пользователь является членом группы A и эта группа вложена в группу B, то права пользователя представляют собой набор прав, назначенных этому пользователю, и прав, назначенных группам A и B. Это означает, что, если вы назначаете права группе B, вложенные группы и пользователи, входящие в группу B, наследуют эти права.

В случае круговой вложенности групп члены круга, а также их дочерние группы не наследуют права, назначенные их родительским группам.

Чтобы назначить роли пользователю или группе домена в тенанте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Права доступа** и выберите **Пользователи** или **Группы** в зависимости от того, кому вы хотите назначить роли.

   Откроется таблица пользователей или групп домена.

4. При необходимости настройте таблицу:

   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

     Фильтр невозможно применить к столбцам **Роли группы** и **Роли родительской группы**.

   - Нажмите значок параметров () для настройки отображения столбцов.

5. Нажмите на кнопку **Добавить пользователя** или на кнопку **Добавить группу** в зависимости от вкладки, выбранном на шаге 3.

6. В открывшемся окне выполните одно из следующих действий:

   a. Если на шаге 3 вы выбрали **Пользователи**, в поле **Пользователь** введите имя пользователя или адрес электронной почты. Если на шаге 3 вы выбрали вкладку **Группы**, в поле **Группа** укажите название группы.

   b. Установите флажки рядом с ролями, которые вы хотите назначить пользователю или группе домена.

      При необходимости вы можете выбрать несколько ролей.

   c. Нажмите на кнопку **Добавить**.

   Окно закроется, пользователь или группа домена отобразятся в списке.

7. Нажмите на кнопку **Сохранить**.

   Пользователь или группа домена, с назначенными ролями, будут добавлены в тенант. При необходимости вы можете изменить роли, нажав на имя пользователя или группу домена и выполнив действия, описанные в шагах 6–7.

Удаление тенантов

За один раз можно удалить только один тенант. Если у выбранного тенанта есть дочерние тенанты, они также будут удалены. Плейбуки, связанные с тенантами, будут удалены, а информация об алертах и инцидентах, связанных с тенантом, станет недоступной.

При удалении тенанта в Консоли OSMP в Консоли KUMA происходят следующие изменения:

- Тенант и его ресурсы удалены. Активы удаленного тенанта архивируются и удаляются по истечении срока действия архивированного актива.
- Части хранилища, относящиеся к тенанту будут удалены.
- Сырые события становятся недоступными.
- Статусы служб удаленных тенантов изменятся на **Серый**.

> Чтобы удалить тенант, у вас должны быть права на **Чтение** и **Запись** в функциональной области **Тенанты** в выбранном тенанте.

Вы не можете удалить корневой тенант и общий тенант, которые были перенесены из Kaspersky Unified Monitoring and Analysis Platform.

Чтобы удалить тенант:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Установите флажок напротив тенанта, который требуется удалить. Если у выбранного тенанта есть дочерние тенанты, они будут выбраны автоматически, и отменить их выбор невозможно.

3. Нажмите на кнопку **Удалить**.

4. Подтвердите операцию, указав имя тенанта, который вы хотите удалить. Если у тенанта есть дочерние тенанты, они также перечислены как тенанты, подлежащие удалению.

Выбранный тенант, его дочерние тенанты (если есть) и связанные объекты удалены.

Настройка параметров отправки уведомлений по электронной почте

Вы можете настроить уведомления по электронной почте о событиях, происходящих в Kaspersky EDR Expert, через Сервер администрирования Kaspersky Security Center и внешний SMTP-сервер. Для этого необходимо настроить параметры подключения к SMTP-серверу.

Чтобы настроить подключение к SMTP-серверу:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Параметры** и нажмите на **Подключение к почтовому серверу**.

4. В правой панели нажмите на кнопку **Просмотреть свойства**.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

   В окне отображаются свойства главного Сервера администрирования и параметры SMTP для главного Сервера администрирования, независимо от того, к какому Серверу администрирования привязан тенант.

5. Настройте параметры, как описано в шаге 2 Настройка параметров доставки уведомлений.

После настройки подключения к SMTP-серверу пользователи начнут получать электронные письма от Kaspersky EDR Expert.

Вы можете создавать шаблоны уведомлений по электронной почте, которые будут отправляться указанным пользователям при обнаружении определенных алертов, инцидентов или событий. Эти шаблоны также можно изменять и удалять.

Создание шаблона уведомления

После настройки уведомлений по электронной почте о событиях, происходящих в Kaspersky EDR Expert, вы сможете создавать собственные шаблоны для этих уведомлений, приходящих по электронной почте.

Чтобы создать шаблоны уведомлений, вам нужно иметь одну из следующих EDR-ролей: Главный администратор, Администратор тенанта или Администратор SOC.

Когда вы разворачиваете Kaspersky EDR Expert, у вас есть шаблоны для уведомлений по электронной почте в корневом тенанте. Если вы создаете дочерний тенант, он автоматически копирует параметры родительского тенанта. Так как параметры дочернего тенанта и родительского не связаны, изменения, которые вы вносите в параметры дочернего тенанта, не влияют на параметры родительского тенанта и наоборот.

Чтобы создать шаблон уведомления по электронной почте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Отобразится список тенантов.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и в разделе **Detection and response** нажмите на **Шаблоны электронных писем**.

   Отобразится таблица типов событий, для которых вы можете настроить шаблоны уведомлений.

4. Если на шаге 2 вы выбрали корневой тенант, в поле **Отображаемое имя Сервера администрирования** укажите адрес, который будет использоваться в ссылках на алерты и инциденты в электронных письмах.

5. Нажмите на кнопку **Создать** и в открывшемся раскрывающемся списке выберите тип события, для которого необходимо создать шаблон уведомления по электронной почте.

6. В открывшейся панели **Создать шаблон электронной почты** укажите следующие параметры:

   Доступные поля зависят от выбранного типа события.

   - В поле **Имя** укажите имя шаблона уведомления по электронной почте.
   - Если вы хотите изменить тип события в шаблоне уведомления по электронной почте, выберите новый тип в поле **Тип события**.
   - Если вы хотите включить уведомление по электронной почте для выбранного типа события, переведите переключатель в положение **Включено** в поле **Статус**.

     Вы также можете включить уведомления по электронной почте из таблицы типов событий. По умолчанию уведомления по электронной почте выключены.

- В поле **Тема** укажите тему электронного письма. Обязательное поле.

  Также вы можете использовать поля алертов, поля инцидентов и нормализованные поля событий KUMA в поле **Тема** – например, `Новый инцидент в OSMP: {{ .InternalID }}, {{ .Name }}`.

- В поле **Шаблон** напишите текст уведомления по электронной почте.

  Пример уведомления по электронной почте

```
Hello,<br>
<br>
Alert {{ .InternalID }}{{ with escapeHTML .Rules.Names }} "{{ . }}"{{ else }}{{ end }} was registered at {{
.CreatedAt }}.<br>
<br>
Details on alert:<br>
<br>
Tenant: {{ .TenantID }}<br>
Alert severity: {{ .Severity }}<br>
Alert first seen: {{ .FirstEventTime }}<br>
Alert last seen: {{ .LastEventTime }}<br>
Full information about the alert is available in OSMP web-interface: {{ link_alert . }}<br>
<br>
Open Single Management Platform
```

  Также вы можете использовать поля алертов, поля инцидентов, нормализованные поля событий KUMA и HTML-теги.

  При написании шаблона вы можете использовать следующие функции:

  - `date` – определяет формат даты и времени. Функция принимает время в миллисекундах (UNIX-время) в качестве первого параметра. Второй параметр можно использовать для передачи времени в формате стандарта RFC. Часовой пояс невозможно изменить.

```
{{range .Events }}
Service name: {{.Event.ServiceName}}
Device host name:  {{.Event.DeviceHostName}}
Message: {{.Event.Message}}
{{end}}
```

> Nested objects can have their own nested objects. You can access them using nested range functions.

  - `limit` – ограничивает количество объектов, возвращаемых функцией `range`.
  - `link_alert` – генерирует ссылку на алерт с указанным URL в поле **Отображаемое имя Сервера администрирования**.
  - `link_incident` – генерирует ссылку на инцидент с указанным URL в поле **Отображаемое имя Сервера администрирования**.
  - `link` – принимает форму ссылки, которую пользователь может открыть, когда он получает уведомление по электронной почте.

- В поле **Получатели** укажите один или несколько адресов электронной почты для отправки уведомлений.

- В раскрывающемся списке **Правила корреляции** выберите одно или несколько правил корреляции, в соответствии с которыми будет отправляться уведомление по электронной почте.

- В поле **Уведомлять в зависимости от уровня критичности** выберите минимальный уровень критичности алерта, при достижении которого будет отправлено уведомление по электронной почте. Для алертов с уровнем критичности ниже указанного уведомление по электронной почте отправлено не будет.

- В раскрывающемся списке **Технологии обнаружения** выберите одну или несколько технологий обнаружения, при обнаружении которых будет отправляться уведомление по электронной почте.

- При необходимости в поле **Описание** напишите описание шаблона уведомления.

7. Нажмите на кнопку **Создать**.

   Окно **Создать шаблон электронной почты** закроется.

8. В окне свойств тенанта сохраните изменения.

Шаблон уведомления по электронной почте будет создан и сохранен. При возникновении выбранных типов событий в Kaspersky EDR Expert на указанные адреса электронной почты будут отправлены соответствующие уведомления.

Изменение и удаление шаблона уведомления

Вы можете изменить или удалить шаблон электронного письма о событиях, происходящих в Kaspersky EDR Expert.

Чтобы изменить или удалить шаблон уведомления, необходима одна из следующих EDR-ролей: Главный администратор, Администратор тенанта или Администратор SOC.

Когда вы разворачиваете Kaspersky EDR Expert, у вас есть шаблоны для уведомлений по электронной почте в корневом тенанте. Если вы создаете дочерний тенант, он автоматически копирует параметры родительского тенанта. Так как параметры дочернего тенанта и родительского не связаны, изменения, которые вы вносите в параметры дочернего тенанта, не влияют на параметры родительского тенанта и наоборот.

Чтобы изменить шаблон уведомления по электронной почте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Отобразится список тенантов.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Параметры** и нажмите **Шаблоны электронных писем**.

4. В таблице в столбце **Тип события** нажмите на тип событий шаблона уведомлений, который вы хотите изменить.

5. В открывшемся окне **Изменить шаблон электронной почты** измените нужные параметры.

6. Сохраните изменения.

   Окно **Изменить шаблон электронной почты** закроется.

7. Сохраните изменения.

Шаблон уведомления по электронной почте будет изменен и сохранен. При возникновении событий выбранных типов в Kaspersky EDR Expert шаблон уведомления будет отправлен на указанные адреса электронной почты.

Чтобы удалить шаблон уведомления по электронной почте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Отобразится список тенантов.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Параметры** и нажмите **Шаблоны электронных писем**.

4. Установите флажок рядом с шаблоном уведомлений, который вы хотите удалить.

5. Нажмите на кнопку **Удалить**.

6. В открывшемся окне подтвердите удаление.

Шаблон уведомления по электронной почте удален.

Настройка автоматической ротации файлов в разделе Файлы

Автоматическая ротация файлов обеспечивается за счет ограничения пространства раздела **Файлы**: при достижении ограничения самые старые файлы удаляются из раздела. Если вы не укажете ограничение, вы не сможете загружать новые файлы в раздел **Файлы** после того, как у вас закончится пространство, выделенное для этого раздела при развертывании Kaspersky EDR Expert.

Например, во время процедуры развертывания для раздела **Файлы** было выделено 20 ГБ дискового пространства. Затем в параметрах тенанта вы указали 10 ГБ в качестве ограничения, при котором самые старые файлы в разделе **Файлы** будут удалены. Если вы не указали ограничение, вы не сможете загружать файлы в раздел **Файлы** при достижении 20 ГБ.

Чтобы настроить автоматическую ротацию файлов в разделе Файлы:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Перейдите на вкладку **Параметры** и в разделе **Ротация файлов** выполните следующие действия:

   a. В поле **Автоматическая ротация файлов** установите переключатель в положение **Включено**.

   b. В поле Максимальный размер хранилища укажите объем файлов, при котором самые старые файлы будут удаляться из раздела **Файлы**.

      Минимальное значение – 1 ГБ.

   c. Нажмите на кнопку **Сохранить** или **Сохранить и закрыть**, чтобы сохранить параметры.

Автоматическая ротация файлов включена и настроена.

Резервное копирование и восстановление данных Kaspersky EDR Expert

Резервное копирование позволяет сохранять полную копию данных Kaspersky EDR Expert. В процессе резервного копирования работа компонентов Kaspersky EDR Expert временно приостанавливается для обеспечения целостности данных. После создания резервная копия сохраняется в сетевой папке на отдельном сервере, после чего решение возобновляет свою работу. Резервное копирование можно создавать вручную или по заданному расписанию.

Следуя этому сценарию, вы можете настроить хранилище резервных копий, настроить расписание для создания резервного копирования или создать резервную копию вручную, а также управлять резервными копиями и восстанавливать данные Kaspersky EDR Expert из резервной копии.

Ограничения:

- В процессе резервного копирования работа компонентов Kaspersky EDR Expert временно приостанавливается для обеспечения целостности данных.
- Резервная копия включает в себя все данные Kaspersky EDR Expert. Создание резервной копии или восстановление данных отдельного компонента не поддерживается.
- Восстановление данных Kaspersky EDR Expert из резервной копии необходимо выполнять с использованием той же версии Kaspersky EDR Expert, в которой была создана резервная копия.
- Резервное копирование и восстановление данных Kaspersky EDR Expert поддерживается только в том случае, если СУБД не включена в кластер Kubernetes. Конфигурация, в которой СУБД установлена в кластер Kubernetes, используется только для ознакомления с решением, а не для решения стандартных рабочих задач.
- Свободное место для резервной копии не проверяется автоматически. Вам нужно убедиться, что в сетевой папке достаточно свободного места.

Этапы

Резервное копирование и восстановление данных Kaspersky EDR Expert состоит из следующих этапов:

1. **Настройка хранилища резервных копий**

   Укажите путь к сетевой папке для хранения резервных копий. Эта сетевая папка должна располагаться на отдельном сервере и быть доступна из кластера Kubernetes с использованием протокола CIFS или NFS.

   Чтобы избежать перегрузки сетевой папки, максимальное количество резервных копий, которые можно хранить в сетевой папке, ограничено. По умолчанию вы можете создать до 10 резервных копий. Вы можете задать максимальное количество резервных копий с помощью параметра `backup_retain` при создании резервной копии вручную или при настройке расписания для создания резервного копирования. Если сетевая папка уже содержит максимальное количество резервных копий, следующая резервная копия перезапишет самую старую.

   Поскольку доступное место в сетевой папке не проверяется автоматически, рекомендуется регулярно контролировать свободное место в этой папке, чтобы предотвратить сбои резервного копирования.

2. **Создание резервной копии данных Kaspersky EDR Expert**

   Для создания резервной копии воспользуйтесь одним из следующих способов:

   - Резервное копирование по расписанию

     Если вы хотите создавать резервные копии по расписанию, вам нужно настроить расписание с помощью KDT. Вы можете задать только одно расписание резервного копирования. Создание нового расписания заменит существующее. Также вы можете просмотреть текущее расписание и приостановить или возобновить автоматическое резервное копирование.

     Перед использованием автоматического запланированного резервного копирования рекомендуется создать резервную копию вручную, чтобы убедиться, что сетевая папка для хранения резервных копий настроена правильно и доступна.

   - Резервное копирование вручную

     Если вам нужно сохранить резервную копию, не дожидаясь следующего запуска автоматического резервного копирования, вы можете создать резервную копию вручную.

   Резервная копия сохраняется в указанной сетевой папке. Вы можете просмотреть список доступных резервных копий и информацию о каждой резервной копии.

   Журналы KDT предоставляют информацию о результатах операции резервного копирования, включая ее успешность или неудачу, дату и время выполнения, а также имя и местоположение резервной копии.

3. **Восстановление данных Kaspersky EDR Expert из резервной копии**

   Восстановите резервную копию данных, чтобы откатить Kaspersky EDR Expert к сохраненному состоянию.

Настройка хранилища для резервной копии Kaspersky EDR Expert

Все созданные резервные копии хранятся в сетевой папке на отдельном сервере. Эта папка должна быть доступна из кластера Kubernetes с использованием протокола CIFS или NFS.

> Свободное место для резервной копии не проверяется автоматически. Вам нужно убедиться, что на сетевом ресурсе достаточно свободного места.

Чтобы избежать перегрузки сетевой папки, максимальное количество резервных копий, которые можно хранить в сетевой папке, ограничено. По умолчанию вы можете создать до 10 резервных копий. Вы можете задать максимальное количество резервных копий с помощью параметра `backup_retain` при создании резервной копии вручную или при настройке расписания для создания резервного копирования. Если сетевая папка уже содержит максимальное количество резервных копий, следующая резервная копия перезапишет самую старую.

Указание пути к сетевой папке для хранения резервных копий

Чтобы указать путь к хранилищу резервных копий, доступный по протоколу CIFS/SMB,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a setBackupStore \
  --param backup_target_url="cifs://<устройство>/<путь>" \
  --param cifs_username="<имя пользователя>" \
  --param cifs_password="<пароль>"
```

где:

- `< устройство >` – адрес сетевого сервера хранения данных.
- `< путь >` – путь к сетевой папке резервной копии.
- `< имя пользователя >` – имя пользователя для доступа к сетевой папке.
- `< пароль >` – пароль для доступа к сетевой папке.

  Если пароль содержит двойные кавычки, используйте обратную косую черту (`\"`).

Чтобы указать путь к хранилищу резервных копий, доступный по протоколу NFS,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a setBackupStore --param backup_target_url="nfs://<устройство>:/<путь>"
```

где:

- `< устройство >` – адрес сетевого сервера хранения данных.
- `< путь >` – путь к сетевой папке резервной копии.

Путь к сетевой папке для хранения резервных копий будет указан.

Просмотр пути к сетевой папке для хранения резервных копий

Чтобы просмотреть текущий путь хранения резервных копий,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a getBackupStore
```

Отобразится текущий путь хранения резервной копии.

Настройка и управление расписанием резервного копирования

Kaspersky EDR Expert позволяет создавать резервные копии данных по расписанию, просматривать текущее расписание, приостанавливать или возобновлять запланированное резервное копирование, а также удалять расписание.

Вы можете настроить только одно расписание резервного копирования. Создание нового расписания заменит существующее.

Перед использованием автоматического запланированного резервного копирования рекомендуется создать резервную копию вручную, чтобы убедиться, что сетевая папка для хранения резервных копий настроена правильно и доступна.

Настройка расписания создания резервной копии

Чтобы настроить расписание создания резервной копии:

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a updateSchedule \
  --param schedule='<schedule>' \
  --param schedule_paused=<schedule_is_paused> \
  --param backup_retain=<max_number_of_backups>
```

где:

- `<schedule>` – строка в формате UNIX cron, которая определяет периодичность резервного копирования. Например, если вы хотите создавать резервную копию в 9:30 утра 1-го и 15-го числа каждого месяца и каждый понедельник, используйте следующую команду:

  `./kdt invoke backup-operator -a updateSchedule --param schedule='30 9 1,15 * 1' --param schedule_paused=false --param backup_retain=5`

  Формат проверяется: при вводе неверного параметра отображается сообщение об ошибке.

- `<schedule_is_paused>` – параметр, который определяет статус запланированного резервного копирования после создания расписания:
  - `<schedule_is_paused>=false` – запланированное резервное копирование активно и будет запущено в соответствии с указанными параметрами.
  - `<schedule_is_paused>=true` – запланированное резервное копирование приостановлено и не будет запущено.
- `<max_number_of_backups>` – максимальное количество резервных копий, которые можно сохранить в сетевой папке. Значение по умолчанию – 10. Если сетевая папка уже содержит максимальное количество резервных копий, следующая резервная копия перезапишет самую старую. Если уменьшить значение параметра (например, установить `<max_number_of_backups>` равным `3` при создании резервной копии вручную или при настройке расписания резервного копирования), KDT удалит все резервные копии, кроме трех самых последних.

Расписание создания резервной копии будет настроено.

Просмотр информации о расписании резервного копирования

Чтобы просмотреть информацию о расписании резервного копирования,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a getBackupSchedule
```

Отобразятся сведения о настроенном расписании резервного копирования, включая название расписания в столбце `NAME`.

Приостановка запланированного резервного копирования

Чтобы приостановить запланированное резервное копирование,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=true
```

Запланированное резервное копирование будет приостановлено.

Возобновление запланированного резервного копирования

Чтобы возобновить запланированное резервное копирование,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=false
```

Запланированное резервное копирование будет возобновлено.

Создание резервной копии данных Kaspersky EDR Expert вручную

Если вам нужно сохранить резервную копию, не дожидаясь следующего автоматического резервного копирования, или убедиться, что сетевая папка для хранения резервных копий настроена правильно и доступна, вы можете создать резервную копию вручную. В процессе резервного копирования работа компонентов Kaspersky EDR Expert временно приостанавливается для обеспечения целостности данных.

Чтобы создать резервную копию вручную,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a createBackup --param backup_retain=
<max_number_of_backups>
```

где `<max_number_of_backups>` – максимальное количество резервных копий, которые можно сохранить в сетевой папке. Значение по умолчанию – 10. Если сетевая папка уже содержит максимальное количество резервных копий, следующая резервная копия перезапишет самую старую. Если уменьшить значение параметра (например, установить `<max_number_of_backups>` равным `3` при создании резервной копии вручную или при настройке расписания резервного копирования), KDT удалит все резервные копии, кроме трех самых последних.

Резервная копия будет сохранена в настроенной сетевой папке. Журналы KDT предоставляют информацию о результатах операции резервного копирования, включая ее успешность или неудачу, дату и время выполнения, а также имя и местоположение резервной копии.

Просмотр резервных копий данных Kaspersky EDR Expert

Просмотр списка резервных копий

Чтобы просмотреть список резервных копий,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a listBackups
```

Отобразится список резервных копий. В списке отображается размер резервной копии, статус, дата и время выполнения резервного копирования, а также имя резервной копии в столбце `NAME` и уникальный идентификатор резервной копии в столбце `BACKUPID`.

Просмотр информации о резервной копии

Чтобы просмотреть информацию о резервной копии,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a describeBackup --param backup_id='<backup_name>'
```

где `<backup_name>` – имя резервной копии данных, которое отображается в столбце `NAME` в списке резервных копий.

Отобразятся сведения о резервной копии.

При необходимости резервные копии можно удалить с помощью пользовательского действия. Для этого на устройстве администратора, на котором расположена утилита KDT, выполните команду:

```
./kdt invoke backup-operator -a deleteBackup --param
backup_id='01kp2qkprmwaajpd8cgy3zeqbt'
```

Восстановление данных Kaspersky EDR Expert из резервной копии

Перед восстановлением данных убедитесь, что вы используете ту же версию Kaspersky EDR Expert, в которой была создана резервная копия.

Резервное копирование и восстановление данных Kaspersky EDR Expert поддерживается только в том случае, если СУБД не включена в кластер Kubernetes. Конфигурация, в которой СУБД установлена в кластер Kubernetes, используется только для ознакомления с решением, а не для решения стандартных рабочих задач.

Чтобы восстановить данные Kaspersky EDR Expert из резервной копии,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a restoreFromBackup --param backup_id='<backup_id>'
```

где `<backup_id>` – уникальный идентификатор резервной копии данных, который отображается в столбце `BACKUPID` в списке созданных резервных копий.

Данные Kaspersky EDR Expert будут восстановлены из резервной копии. В файлах журнала KDT выводит информацию об успехе или неудаче операции восстановления и ее общей продолжительности.

Чтобы посмотреть статус восстановления данных Kaspersky EDR Expert из резервной копии,

На устройстве администратора выполните команду:

```
./kdt invoke backup-operator -a restoreStatus
```

Kaspersky EDR Expert API

Kaspersky EDR Expert позволяет работать с REST API и OpenAPI.

Работа с REST API

Используя API, вы можете получить доступ к Kaspersky EDR Expert из решений сторонних производителей. REST API работает по протоколу HTTP и состоит из набора методов запросов/ответов.

Справка REST API Swagger: EDR

Справка REST API Swagger: KUMA

На странице Swagger используйте раскрывающийся список **Выбрать определение** для переключения между наборами API KUMA и API EDR (OSMP).

Запросы REST API необходимо отправлять по следующему адресу:

https://<api_host>.<smp_domain>/xdr/api/v1/<request>

https://<api_host>.<smp_domain>/xdr/api/v3/kuma/<request> (для API, специфичного для KUMA)

Где параметр <smp_domain> – это доменное имя сервиса, указанное в конфигурационном файле при развертывании Kaspersky EDR Expert.

Пример:

https://api.example.com/xdr/api/v1/

https://api.example.com/xdr/api/v3/kuma/ (для API, специфичного для KUMA)

Поскольку запросы REST API требуют авторизации, необходимо создать токен.

Работа с OpenAPI

OpenAPI позволяет автоматизировать и настроить управление Сервером администрирования с помощью скриптов. OpenAPI также можно использовать для разработки пользовательских клиентских приложений, которые взаимодействуют с Kaspersky EDR Expert по протоколу HTTP с помощью синхронных запросов и ответов на основе JSON.

Запросы OpenAPI необходимо отправлять по следующему адресу:

https://api.<smp_domain>:13299

Где параметр <smp_domain> – это доменное имя сервиса, указанное в конфигурационном файле при развертывании Kaspersky EDR Expert.

Пример:

https://api.example.com:13299

Методы API, недоступные по лицензии EDR

По лицензии EDR недоступны следующие методы:

- Методы управления активами:
  - `GET /xdr/api/v3/kuma/assets`
  - `POST /xdr/api/v3/kuma/assets/import`
  - `POST /xdr/api/v3/kuma/assets/delete`
- Методы управления параметрами:
  - `GET /xdr/api/v3/kuma/settings/id/{id}`
  - `GET /xdr/api/v3/kuma/settings/extendedFields/export`
  - `POST /xdr/api/v3/kuma/settings/extendedFields/import`
- Методы управления службами:
  - `POST /xdr/api/v3/kuma/services/create`
- Методы управления инцидентами:
  - `GET /xdr/api/v1/incident/workflows/tenants`
  - `GET /xdr/api/v1/incidents/types/usage`

Создание токена

Чтобы сгенерировать пользовательский API-токен:

1. В главном окне приложения перейдите в раздел **Параметры** → **API-токены**.
2. Нажмите на кнопку **Добавить токен**.

3. В панели **Добавить токен** настройте параметры токена.

   a. Нажмите на **Дата истечения срока действия** и используйте календарь, чтобы указать дату истечения срока действия токена. Если вы хотите выключить автоматическое истечение срока действия токена, установите флажок **Без срока действия**.

      Максимальный срок действия – 365 дней.

      > Рекомендуется включить автоматическое истечение срока действия для токенов, у которых есть доступ к методам POST.

   b. Установите флажки рядом с методами API, к которым вы хотите разрешить доступ.

      Кроме методов API вы можете выбрать цели создания токена:

      - POST:DynamicClientRegistration – Динамическая регистрация клиентов OAuth.
      - POST:KSCOpenAPI – Аутентификация в OpenAPI с использованием API-токенов.

4. Нажмите на кнопку **Сгенерировать**.

5. Нажмите на кнопку **Копировать и закрыть**.

   > Вы не сможете скопировать токен позже.

Токен создан и скопирован в буфер обмена. Сохраните токен любым удобным способом.

Авторизация запросов API

Каждый запрос API должен включать авторизацию с использованием токенов. Пользователь, чей токен используется для запроса API, должен иметь разрешения на выполнение этого типа запроса.

Каждый запрос должен сопровождаться следующим заголовком:

```
Authorization: Bearer <token>
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`
400	Неверный заголовок.	Неверный заголовок авторизации.
403	Токен не существует или пользователь (владелец токена) выключен.	Доступ запрещен.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Open Single Management Platform, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Open Single Management Platform.

Kaspersky предоставляет поддержку Open Single Management Platform в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Известные проблемы и ограничения

Увеличены минимальные аппаратные требования по сравнению с предыдущей версией решения Kaspersky EDR Expert. Для работы решения требуется процессор не менее 12 ядер и оперативная память не менее 32 ГБ.

Ограничения OSMP

Для OSMP действуют следующие ограничения:

- 10721464: При отключении EDR и переносе актива в KATA в таблице активов (**Активы (Устройства)** → **Обнаружение и реагирование**) у перенесенного актива сохраняется параметр "EDR" в столбце **Источник актива**. Это может препятствовать выполнению реагирования KATA.
- 9495472: Если вы планируете использовать несколько тенантов в своей инфраструктуре, создайте отдельный коллектор для каждого тенанта.
- 9792316: В окне свойств Сервера администрирования на вкладке **Двухфакторная аутентификация** отображается таблица **Пользователям разрешено генерировать секретные ключи**. Поскольку всем пользователям разрешено генерировать секретные ключи, таблица не имеет смысла.
- 7208621: При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.
- 6822204: Уведомления о новых версиях доступных для загрузки веб-плагинов отключены. Вы можете обновить плагины с помощью Kaspersky Deployment Toolkit.
- 6919635: После создания нового тенанта алерты, связанные с ним, отправляются на сервер, но не отображаются в таблице алертов. Вам может потребоваться обновить веб-страницу, чтобы обновить данные таблицы.
- Действие ответа Получить метафайлы NTFS не возвращает альтернативные потоки запрошенных метафайлов, если их основной поток отсутствует.
- Действие "Запустить ответ приложения" на устройствах Linux не позволяет использовать подстановочные знаки (в частности, символ "*") в пути к файлу.
- Для развертывания приложения на виртуальной платформе KVM вам необходимо установить гипервизор KVM на базе операционной системы Debian GNU/Linux 12 с использованием эмулятора QEMU version 8.0.2.
- Перенос данных напрямую из Kaspersky EDR Expert 7.1 в версию 8.2 не поддерживается. Требуется перенести данные в Kaspersky EDR Expert 8.1, а затем обновить решение до версии 8.2.
- 10419403: С помощью веб-интерфейса или API Kaspersky EDR Expert можно получить и экспортировать до 1000 событий поиска угроз.

- 10079501: При использовании иерархии экземпляров права, назначенные в Kaspersky Security Center, не реплицируются с родительского экземпляра на дочерние экземпляры. Чтобы обеспечить правильную работу, назначьте вручную необходимые права реплицированным пользователям на каждом дочернем экземпляре.

- 10042351: Если вы получили дамп памяти для процесса с объемом памяти 3 ГБ или более, действие по реагированию запускается, но не завершается.

- 10421874: Для уменьшения размера хранилища во всех нормализаторах отключены сырые журналы, поэтому запросы не могут выполнять поиск по всем полям событий.

- 10420850: После синхронизации Active Directory при входе в Консоль OSMP может отображаться сообщение об ошибке при конфигурации, а перезагрузка может привести к ошибке `Нет исправных вышестоящих узлов`.

- 10420739: В базе Сервера администрирования могут возникнуть проблемы со свободным местом из-за циклической зависимости доменных групп.

- 10419715: KUMA в OSMP не поддерживает лицензию Kaspersky Smart II. Для использования этой лицензии разверните KUMA как отдельный компонент и Kaspersky EDR Expert отдельно.

- 10408974: При использовании пакета KIAkOAPI токен аутентификации предъявителя не указан в заголовках запросов, что может привести к сбою вызовов API с ошибкой `401 Unauthorized`. Пользовательский токен предъявителя потребуется вручную добавить в заголовок авторизации.

- 10408469: Не поддерживается интеграция с Kaspersky Endpoint Agent 3.16 и 4.0.

- 10404511: Если плейбук включает действие, на которое не распространяется текущая лицензия, он будет помечен как недоступный.

- 10403607: Когда интеграция с Kaspersky Security Center включена, периодические прерывания связи могут препятствовать доступу вторичного Сервера администрирования к первичному Серверу администрирования. Кроме того, в разделе **Активы (Устройства)** будет доступна только вкладка **Общие**, а другие вкладки будут недоступными. Рекомендуется проверить, верно ли указаны параметры подключения и сертификаты на каждом Сервере администрирования, а также правильность настройки иерархии.

- 10360014: Если сырые события недоступны, вы можете просмотреть значения полей в веб-интерфейсе. Имена полей сырых событий полностью соответствуют тем, которые отображаются в веб-интерфейсе. С подробными описаниями полей можно ознакомиться в справке.

- Невозможно создать коллектор без лицензии Kaspersky Symphony XDR.

- Экспорт сырых данных телеметрии без лицензии Kaspersky Symphony XDR производится некорректно.

Ограничения Sandbox

Для компонента Sandbox действуют следующие ограничения:

- По умолчанию максимальный размер файла, проверяемого модулем Sandbox, составляет 100 МБ. Параметры проверки можно настроить в меню администратора консоли управления приложением.
- Максимальный уровень вложенности проверяемых архивов составляет 32.
- Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 20 тысяч объектов. По достижении этого ограничения приложение удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в приложении со статусом NOT_SCANNED (непроверенные).

Глоссарий

Bootstrap

Базовая среда выполнения, включающая кластер Kubernetes и компоненты инфраструктуры для работы Kaspersky EDR Expert. Bootstrap входит в транспортный архив и автоматически устанавливается при развертывании Kaspersky EDR Expert.

EPP-программа

Программа устанавливается на конечные устройства для обеспечения защиты и передачи отчетов о ее состоянии Серверу администрирования, который занимается централизованным управлением. Для Kaspersky EDR Expert приложениями EPP являются Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Mac.

IOA-правило

Kaspersky EDR Expert использует индикаторы атаки (IOA). IOA-правила содержат описание подозрительной активности в системе, которая может быть признаком целевой атаки. Эти правила скачаны из репозитория KUMA и используются технологией TAA (Targeted Attack Analyzer) для поиска угроз. Вы можете открыть сведения о IOA-правиле из соответствующих сведений алерта. Также в Консоли OSMP есть предустановленное IOA-правило. Предустановленное IOA-правило отображается в таблице правил корреляции: **Мониторинг** → **Ресурсы и сервисы** → **Правила корреляции**. Если срабатывает предустановленное IOA-правило, создаются IOA-алерты.

IOC-файл

IOC файлы содержат набор индикаторов, которые сравниваются с индикаторами события. Если сравниваемые индикаторы совпадают, приложение считает событие обнаружением и создает алерт. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Kaspersky Deployment Toolkit

Утилита, используемая для развертывания и управления кластером Kubernetes, компонентами Kaspersky EDR Expert и веб-плагинами управления. KDT работает на устройстве администратора и подключается к целевым устройствам с помощью SSH.

Lightweight Nagent (LWNGT)

Протокол взаимодействия с Kaspersky Endpoint Security на мобильных устройствах. Протокол LWNGT (также мобильный протокол) выполняет роль Агента администрирования без фактической установки Агента администрирования на мобильные устройства.

Network Location Awareness (NLA)

Служба Windows, которая помогает операционной системе идентифицировать текущую сеть. NLA обнаруживает изменения в сети и настраивает конфигурацию безопасности устройства.

Агент

Службы KUMA, которые используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

Агент администрирования

Open Single Management Platform – это компонент, обеспечивающий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех приложений, разработанных для систем Microsoft® Windows®. Для приложений "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.

Актив

Устройство или пользователь защищаемой инфраструктуры. Если на активе обнаружен алерт или инцидент, вы можете выполнить действия по реагированию для этого актива.

Алгоритм плейбука

Алгоритм, включающий последовательность действий по реагированию, которые помогают анализировать и обрабатывать алерты или инциденты.

Алерт

Событие в ИТ-инфраструктуре организации, которое было отмечено Open Single Management Platform как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуре организации.

Граф расследования

Инструмент для визуального анализа, который показывает отношения между событиями, алертами, инцидентами, наблюдаемыми объектами и активами (устройствами). На графе расследования отображается подробная информация об инциденте: соответствующие алерты, пользователи, активы и их общие свойства.

Действия по реагированию

Действия, запускаемые в плейбуках.

Дистрибутив

Архив, содержащий транспортный архив с компонентами Kaspersky EDR Expert и Лицензионными соглашениями для Kaspersky EDR Expert и KDT, а также архив с утилитой KDT и шаблонами конфигурационного файла и файлом инвентаря KUMA.

Инцидент

Контейнер алертов, который обычно указывает на истинно положительное обнаружение проблемы в ИТ-инфраструктуре организации. Инцидент может содержать один или несколько алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему.

Кластер Kubernetes

Набор устройств, объединенных с помощью Kubernetes в один вычислительный ресурс. Кластер Kubernetes используется для работы компонентов Kaspersky EDR Expert (кроме сервисов KUMA). Кластер Kubernetes может включать в себя как целевые устройства, так и устройство администратора.

Коллектор

Сервис KUMA, который получает сообщения от источников событий, обрабатывает их, а затем передает их в хранилище, коррелятор и/или сторонние службы для идентификации алертов.

Контекст

Набор параметров доступа, определяющих кластер Kubernetes, с которым пользователь может выбрать взаимодействие. Контекст также включает данные для подключения к кластеру с помощью KDT.

Конфигурационный файл

Файл в формате YAML, содержащий список целевых устройств для развертывания Kaspersky EDR Expert и набор параметров для установки компонентов Kaspersky EDR Expert. Конфигурационный файл используется KDT.

Коррелятор

Сервис KUMA, анализирующий нормализованные события.

Маршрутизатор событий

Сервис KUMA, который позволяет принимать потоки событий от коллекторов и корреляторов и далее распределять события по заданным точкам назначения в соответствии с настроенными фильтрами.

Мультитенантность

Режим, который позволяет главному администратору предоставлять функциональность Kaspersky EDR Expert нескольким клиентам независимо или разделять активы и параметры приложения и объекты для разных офисов. Также режим мультитенантности позволяет копировать и наследовать параметры и объекты тенанта от родительского тенанта, а также автоматически распространять лицензионный ключ Kaspersky EDR Expert для всех тенантов в иерархии.

Наблюдаемые объекты

Объекты, связанные с алертом и инцидентом, такие как хеши MD5 и SHA256, IP-адрес, веб-адрес, имя домена, имя пользователя или имя устройства.

Нормализованное событие

Событие, которое обрабатывается в соответствии с нормализованной моделью данных событий KUMA.

Плейбук

Объект, который реагирует на алерты или инциденты в соответствии с заданным алгоритмом (алгоритмом плейбука). Плейбуки позволяют автоматизировать рабочие процессы и сокращать время, необходимое для обработки алертов и инцидентов.

Получить данные для расследования

Набор методов и технологий, направленных на выявление, получение и анализ данных, которые могут быть использованы в качестве цифрового доказательства кибератак или других незаконных действий, осуществляемых на устройствах.

Пользовательские действия

KDT – это команда, позволяющая выполнять дополнительные операции, специфичные для компонентов Kaspersky EDR Expert.

Правила сегментации

Правила, которые позволяют автоматически разделять связанные алерты на отдельные инциденты в зависимости от заданных условий.

Правило корреляции

Ресурс KUMA, используемый для распознавания определенных последовательностей обработанных событий и выполнения заданных действий после распознавания.

Реестр

Компонент инфраструктуры, в котором хранятся контейнеры приложений и который используется для установки и хранения компонентов Kaspersky EDR Expert.

Сервисы KUMA

Основные компоненты KUMA, которые помогают системе управлять событиями. Службы позволяют получать события из источников событий и в дальнейшем приводить их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа. К сервисам KUMA относятся коллекторы, корреляторы и хранилища.

Событие

События информационной безопасности, зарегистрированные на контролируемых элементах ИТ-инфраструктуры организации. Например, события включают попытки входа в систему, взаимодействия с базой данных и многоадресную рассылку информации. Каждое отдельное событие может показаться неинформативным, но, если рассматривать их вместе, они формируют более широкую картину сетевой активности, которая помогает идентифицировать угрозы безопасности.

Тенант

Логический объект, соответствующий организационной единице (клиенту или офису), которой предоставляется функциональность Kaspersky EDR Expert. Каждый тенант может включать в себя активы, пользователей и их права доступа, события, алерты, инциденты, плейбуки, а также интеграцию с другими приложениями, службами и решениями "Лаборатории Касперского". Также тенант определяет набор доступных операций с включенными объектами.

Транспортный архив

Архив, который содержит компоненты Kaspersky EDR Expert и веб-плагинов управления и Лицензионные соглашения Kaspersky EDR Expert и KDT. Транспортный архив включен в дистрибутив.

Узел

Физическая или виртуальная машина, на которой будет развернут Kaspersky EDR Expert. Есть первичный и рабочий узлы. Первичный узел предназначен для управления кластером, хранения метаданных и распределения рабочей нагрузки. Рабочие узлы предназначены для выполнения рабочей нагрузки компонентов Kaspersky EDR Expert.

Устройство администратора

Физическая или виртуальная машина, которая используется для развертывания и управления кластером Kubernetes и Kaspersky EDR Expert с помощью KDT. KDT работает на устройстве администратора. Если устройство администратора не включено в кластер Kubernetes, оно будет использоваться только для развертывания. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Kaspersky EDR Expert.

Файл инвентаря KUMA

Файл в формате YAML, который содержит параметры для установки сервисов KUMA, не включенных в кластер Kubernetes. Путь к файлу инвентаря KUMA включен в конфигурационный файл, который используется KDT для развертывания Kaspersky EDR Expert.

Хранилище

Сервис KUMA, который используется для хранения нормализованных событий, чтобы к ним можно было быстро и постоянно получать доступ из KUMA с целью извлечения аналитических данных.

Целевые устройства

Физические или виртуальные машины, на которых устанавливается Kaspersky EDR Expert. Целевые устройства включены в кластер Kubernetes. Компоненты Kaspersky EDR Expert работают на этих устройствах.

Цепочка развития угрозы

Последовательность шагов, позволяющих отслеживать стадии кибератаки. Цепочка развития угроз позволяет проанализировать причины возникновения угрозы. Для создания цепочки развития угрозы управляемое приложение передает данные с устройства на Сервер администрирования с помощью Агента администрирования.

Информация о стороннем коде

Информация о стороннем коде содержится в файлах legal_notices_ksmp.txt и legal_notices_kuma.txt на устройстве, которое выступает в роли узла оператора. Файлы находятся в директории `~/kaspersky_eula` пользователя, который запускает установку Kaspersky EDR Expert.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD и AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Apache и Apache Cassandra являются либо зарегистрированными товарными знаками, либо товарными знаками Apache Software Foundation в Соединенных Штатах и/или других странах.

Mac и macOS – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

LTS и Ubuntu являются зарегистрированными товарными знаками Canonical Ltd.

Check Point NGFW – товарный знак или зарегистрированный товарный знак Check Point Software Technologies Ltd. или аффилированных компаний.

Cisco, IOS и Snort являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

ClickHouse является зарегистрированным товарным знаком ClickHouse, Inc. https://clickhouse.com/

Citrix и Citrix NetScaler являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

Dell Technologies, Dell и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Elasticsearch – зарегистрированный в США и других странах товарный знак Elasticsearch BV.

ESET является товарным знаком или зарегистрированным товарным знаком ESET spol. s r.o. или соответствующей компании ESET.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.

Firebird – зарегистрированный товарный знак Firebird Foundation.

Fortinet, FortiGate, FortiMail, FortiSOAR – товарные знаки или зарегистрированные в США и/или других странах товарные знаки Fortinet, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Android, Chrome, Firebase, Google Chrome, Google Public DNS – товарные знаки Google LLC.

Huawei Eudemon является товарным знаком Huawei Technologies Co., Ltd.

ViPNet является зарегистрированным товарным знаком компании "ИнфоТеКС".

IBM, Guardium, InfoSphere, QRadar – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Insider, Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

Node.js – товарный знак Joyent, Inc.

Juniper, Juniper Networks и JUNOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Juniper Networks, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Microsoft, Access, Active Directory, BitLocker, Excel, Halo, Hyper-V, Internet Explorer, Lync, Microsoft 365, Microsoft Edge, MS-DOS, Office 365, PowerShell, SharePoint, Skype, SQL Server, Windows, Windows PowerShell, Windows Server и Windows Vista являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla, Firefox являются товарными знаками Mozilla Foundation в США и других странах.

NetApp – товарный знак или зарегистрированный в США и/или других странах товарный знак NetApp, Inc.

Netskope, логотип Netskope и другие названия продуктов Netskope, упомянутые в настоящем документе, являются товарными знаками Netskope, Inc. и/или одной из ее дочерних компаний и могут быть зарегистрированы в Ведомстве по патентам и товарным знакам США и в других странах.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Oracle и JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Chef – товарный знак или зарегистрированный в США и/или других странах товарный знак Progress Software Corporation и/или одной из дочерних или аффилированных компаний.

Puppet – товарный знак или зарегистрированный товарный знак Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

Red Hat, CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Sendmail и другие наименования и названия продуктов – товарные знаки или зарегистрированные товарные знаки Sendmail, Inc.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SolarWinds – товарный знак, права на который принадлежат компании SolarWinds Worldwide, LLC или аффилированным лицам компании, зарегистрирован в Бюро по патентам и товарным знакам США, а также может быть зарегистрирован или находиться в процессе регистрации в других странах.

Splunk – товарный знак и зарегистрированный в США и других странах товарный знак Splunk, Inc.

Название CommuniGate Pro – товарный знак или зарегистрированный товарный знак Stalker Software, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

OpenAPI – товарный знак компании The Linux Foundation.

Trend Micro является товарным знаком или зарегистрированным товарным знаком Trend Micro Incorporated.

Наименования, изображения и логотипы, идентифицирующие продукты и услуги UserGate, являются фирменными знаками UserGate и/или ее дочерних компаний или филиалов, а сами продукты являются собственностью UserGate.

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere, VMware Workstation – зарегистрированные товарные знаки и/или товарные знаки VMware, Inc. в США и других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.

The MITRE Corporation Terms of Use

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.