kaspersky

Kaspersky Unified Monitoring and Analysis Platform

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Unified Monitoring and Analysis Platform

О решении

- Что нового
- Комплект поставки
- Аппаратные и программные требования
- Интерфейс KUMA
- Совместимость с другими программами

Архитектура решения

- Ядро
- Коллектор
- Коррелятор
- Хранилище
- Основные сущности
  - Тенант
  - Событие
  - Алерт
  - Инцидент
  - Активы
  - Ресурсы
  - Сервисы KUMA
  - Агенты KUMA
  - Уровни важности

Лицензирование решения

- О Лицензионном соглашении
- О лицензии
- О Лицензионном сертификате
- О лицензионном ключе
- О файле ключа
- О коде активации
- Предоставление данных в Kaspersky Unified Monitoring and Analysis Platform
- Добавление лицензионного ключа
- Просмотр информации о добавленном лицензионном ключе
- Удаление лицензионного ключа

Руководство администратора

- Установка и удаление KUMA
  - Требования к установке решения
    - Обновление Oracle Linux 8.x до Oracle Linux 9.x с установленными сервисами KUMA
  - Порты, используемые KUMA при установке
  - Скачивание CA-сертификатов
  - Перевыпуск внутренних CA-сертификатов
  - Изменение самоподписанного сертификата веб-консоли
  - Синхронизация времени на серверах

О файле инвентаря
Параметры конфигурации KUMA в файле инвентаря
Установка на одном сервере
Подготовка файла инвентаря single.inventory.yml
Установка KUMA на одном сервере
Изменение имени хоста
Распределенная установка
Подготовка контрольной машины
Подготовка целевой машины
Подготовка файла инвентаря distributed.inventory.yml
Установка KUMA в распределенной конфигурации
Изменение имени хоста микросервисов
Распределенная установка с Ядром KUMA в кластере Kubernetes
Дополнительные требования при развертывании Ядра в Kubernetes
Установка KUMA в кластере Kubernetes
Подготовка контрольной машины
Подготовка целевой машины
Подготовка файла инвентаря k0s.inventory.yml
Установка с Ядром KUMA в кластере Kubernetes
Перенос Ядра KUMA в новый кластер Kubernetes
Доступность Ядра KUMA при различных сценариях
Управление Kubernetes и доступ к KUMA
Часовой пояс в кластере Kubernetes
Обслуживание хостов в кластере Kubernetes
Восстановление кластера Kubernetes
Составляющие части кластера Kubernetes и использование снимков их виртуальных машин
Сценарии сбоев
Распределенная установка с Ядром KUMA в кластере Raft
Подготовка контрольной машины
Подготовка целевой машины
Подготовка файла инвентаря distributed.inventory.yml для установки KUMA с несколькими сервисами Ядра KUMA в кластере Raft
Установка в отказоустойчивой конфигурации в кластере Raft
Настройка балансировщика для кластера Raft
Пример настройки HAProxy Community Edition
Пример настройки NGINX Open Source
Расширение кластера Raft
Удаление узла кластера Raft
Восстановление узла кластера Raft
Восстановление кластера Raft
Восстановление кластера Raft из текущего состояния узла
Восстановление кластера Raft из резервной копии
Изменение имени хоста Ядра KUMA
Резервное копирование KUMA
Создание резервной копии Ядра KUMA
Восстановление Ядра KUMA для установки на одном сервере
Восстановление Ядра KUMA для распределенной установки

Восстановление Ядра KUMA в кластере Kubernetes
Восстановление Ядра KUMA в кластере Raft
Изменение конфигурации KUMA
Обновление предыдущих версий KUMA
Обновление компонентов кластера Kubernetes
Обновление компонентов кластера Kubernetes без параметра -e 'manual_restore_only=true'
Обновление компонентов кластера Kubernetes с параметром -e 'manual_restore_only=true'
Определение размера данных метрик в установке с Ядром KUMA в кластере Kubernetes версии 3.4.x
Увеличение размера тома Ядра KUMA или тома сервиса Метрики в действующем кластере Kubernetes
Уменьшение размера тома сервиса Метрики
Уменьшение размера тома сервиса Метрики без потери данных
Уменьшение размера тома сервиса Метрики с потерей данных
Миграция событий алертов в ClickHouse после обновления KUMA с версии 3.4.x
Параметры миграции событий алертов из MongoDB в ClickHouse
Устранение ошибок при обновлении
Перевыпуск сертификатов кластера k0s при истечении срока действия
Удаление KUMA
Работа с тенантами
Выбор тенанта
Правила принадлежности к тенантам
Управление пользователями
Роли пользователей
Права предустановленных ролей
Создание пользовательской роли
Функциональные области и доступные им уровни полномочий
Изменение параметров пользовательской роли
Просмотр параметров роли
Удаление пользовательской роли
Настройка политики безопасности при входе в веб-интерфейс
Создание учетной записи пользователя
Изменение учетной записи пользователя
Особенности изменения набора пространств, назначенных пользователю
Сервисы KUMA
Инструменты сервисов
Изменение названия сервиса
Получение идентификатора сервиса
Остановка, запуск и проверка статуса сервиса
Перезапуск сервиса
Удаление сервиса
Просмотр таблицы разделов хранилища
Просмотр таблицы активных запросов
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 сервиса хранилища в веб-интерфейсе
Установка хранилища в сетевой инфраструктуре KUMA
Рекомендации по использованию системной памяти
Резервное копирование, восстановление и импорт партиций
Резервное копирование партиций по расписанию
Резервное копирование партиций вручную
Восстановление партиций из резервной копии
Импорт партиций из сторонней установки KUMA
Создание коррелятора
Запуск мастера установки коррелятора
Шаг 1. Общие параметры коррелятора
Шаг 2. Глобальные переменные
Шаг 3. Корреляция
Шаг 4. Обогащение
Шаг 5. Реагирование
Шаг 6. Маршрутизация
Шаг 7. Проверка параметров
Установка коррелятора на сервере
Проверка правильности установки коррелятора
Создание коррелятора correlator-ng
Настройка конфигурации correlator-ng
Развертывание correlator-ng в кластере Raft
Поддерживаемые типы данных correlator-ng
Селекторы правил корреляции и выражения
Атрибуты правила корреляции standard
Функции обработки данных в correlator-ng
Создание маршрутизатора событий
Запуск мастера установки маршрутизатора событий
Шаг 1. Общие параметры маршрутизатора событий
Шаг 2. Маршрутизация
Шаг 3. Проверка параметров
Установка маршрутизатора событий на сервере
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 событий
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 агента
Создание набора ресурсов для агента
Управление подключениями для агента
Создание сервиса агента в веб-интерфейсе KUMA
Автоматически созданные агенты
Установка агента в сетевой инфраструктуре KUMA
Установка агента KUMA на устройствах Linux
Установка агента KUMA на устройствах Windows
Обновление агентов
Передача в KUMA событий из изолированных сегментов сети
Конфигурационный файл diode-агента
Описание полей секретов
Установка Linux-агента в изолированном сегменте сети
Установка Windows-агента в изолированном сегменте сети
Передача в KUMA событий с машин Windows
Импорт файла со списком серверов для агентов WMI
AI-сервисы
AI рейтинг и AI-статус активов
Установка и удаление сервиса AI-рейтинг и AI-статус активов
Перевыпуск сертификата AI-сервиса
Параметры настройки сервиса AI-рейтинг и AI-статус активов
Проанализировать с помощью KIRA
Настройка интеграции с KIRA
Выполнение анализа с помощью KIRA
Возможные ошибки задачи Проанализировать с помощью KIRA
Настройка обнаружения атак DLL Hijacking
Сервис Метрики
Установка сервиса Метрики на хосте
Настройка источников событий
Настройка получения событий Auditd
Настройка коллектора KUMA для получения событий Auditd
Настройка сервера источника событий с помощью сервиса rsyslog
Настройка сервера источника событий с помощью сервиса syslog-ng
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
Настройка передачи событий Kaspersky Security Center в SIEM-систему KUMA
Настройка передачи событий Kaspersky Security Center в формате CEF
Настройка коллектора KUMA для сбора событий Kaspersky Security Center
Установка коллектора KUMA для сбора событий Kaspersky Security Center

Настройка получения событий Kaspersky Security Center из MS SQL
Создание учетной записи в MS SQL
Настройка службы SQL Server Browser
Создание секрета в KUMA
Настройка коннектора
Настройка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL
Установка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL
Настройка получения событий с устройств Windows с помощью Агента KUMA (WEC)
Настройка аудита событий с устройств Windows
Настройка политики аудита на устройстве Windows
Настройка аудита с помощью групповой политики
Настройка централизованного получения событий с устройств Windows с помощью службы Windows Event Collector
Настройка передачи данных с сервера источника событий
Настройка сервиса получения событий Windows
Предоставление прав для просмотра событий Windows
Предоставление прав входа в качестве службы
Настройка коллектора KUMA для получения событий с устройств Windows
Установка коллектора KUMA для получения событий с устройств Windows
Настройка передачи в KUMA событий с устройств Windows с помощью Агента KUMA (WEC)
Настройка получения событий с устройств Windows с помощью Агента KUMA (WMI)
Настройка параметров аудита для работы с KUMA
Настройка аудита с помощью локальной политики
Настройка аудита с помощью групповой политики
Настройка передачи данных с сервера источника событий
Предоставление прав для просмотра событий Windows
Предоставление прав входа в качестве службы
Настройка получения событий DNS-сервера с помощью агента ETW
Настройка на стороне Windows
Настройка получения событий PostgreSQL
Установка плагина pgAudit
Настройка Syslog-сервера для отправки событий
Настройка получения событий ИВК Кольчуга-К
Настройка передачи событий ИВК Кольчуга-К в KUMA
Настройка получения событий КриптоПро NGate
Настройка передачи событий КриптоПро NGate в KUMA
Настройка получения событий Ideco UTM
Настройка передачи событий Ideco UTM в KUMA
Настройка получения событий KWTS
Настройка получения событий KLMS
Настройка передачи событий KLMS в KUMA
Настройка получения событий KSMG
Настройка получения событий KICS for Networks
Создание коннектора KICS for Networks для передачи событий в KUMA
Настройка передачи событий KICS for Networks в KUMA
Создание коллектора KUMA для получения событий KICS for Networks

Настройка получения событий PT NAD
Настройка передачи событий PT NAD в KUMA
Настройка получения событий с помощью плагина MariaDB Audit Plugin
Настройка плагина MariaDB Audit Plugin для передачи событий MySQL
Настройка плагина MariaDB Audit Plugin для передачи событий MariaDB
Настройка Syslog-сервера для отправки событий
Настройка получения событий СУБД Apache Cassandra
Настройка журналирования событий Apache Cassandra в KUMA
Настройка получения событий FreeIPA
Настройка передачи событий FreeIPA в KUMA
Настройка получения событий VipNet TIAS
Настройка передачи событий VipNet TIAS в KUMA
Настройка получения событий Nextcloud
Настройка аудита событий Nextcloud
Настройка Syslog-сервера для отправки событий Nextcloud
Настройка получения событий Snort
Настройка журналирования событий Snort
Настройка получения событий Suricata
Настройка аудита событий Suricata
Настройка получения событий FreeRADIUS
Настройка аудита событий FreeRADIUS
Настройка Syslog-сервера для отправки событий FreeRADIUS
Настройка получения событий VMware vCenter
Настройка подключения к VMware vCenter
Настройка получения событий zVirt
Настройка передачи событий zVirt
Настройка получения событий Zeek IDS
Преобразование формата журнала событий Zeek IDS
Настройка получения событий Windows с помощью Kaspersky Endpoint Security для Windows
Настройка получения событий Linux с помощью Kaspersky Endpoint Security для Linux
Настройка получения событий Codemaster Mirada
Настройка аудита системы Codemaster Mirada
Настройка получения событий Postfix
Настройка Postfix для отправки событий
Настройка коллектора KUMA для получения и обработки событий Postfix
Настройка получения событий CommuniGate Pro
Настройка CommuniGate Pro для отправки событий
Настройка коллектора KUMA для получения и обработки событий CommuniGate Pro
Настройка получения событий Yandex Cloud
Настройка аудита событий Yandex Cloud
Настройка передачи событий Yandex Cloud
Настройка получения событий Microsoft 365
Настройка получения событий АПКШ Континент
Подготовительные действия для получения событий АПКШ Континент
Настройка утилиты kuma-kont
Запуск и управление сервисом утилиты kuma-kont
Параметры конфигурационного файла kuma-kont-config.yaml

Настройка получения событий VK WorkSpace Mail
Настройка отправки событий VK WorkSpace Mail
Настройка получения событий Angie
Настройка передачи событий Angie
Настройка получения событий Dallas Lock 8
Настройка отправки событий Dallas Lock 8
Настройка получения событий Единый центр управления Dallas Lock
Настройка отправки событий ЕЦУ Dallas Lock
Настройка получения событий ProFTPD
Настройка аудита событий ProFTPD
Настройка syslog-сервера для отправки событий ProFTPD
Настройка получения событий Vsftpd
Настройка аудита событий Vsftpd
Настройка syslog-сервера для отправки событий Vsftpd
Настройка получения событий HAProxy
Настройка передачи событий HAProxy
Настройка получения событий Veeam Backup & Replication
Настройка передачи событий Veeam Backup & Replication
Настройка получения событий Apache Tomcat
Настройка аудита событий Apache Tomcat
Настройка syslog-сервера для отправки событий Apache Tomcat
Мониторинг источников событий
Состояние источников
Список источников событий
Политики мониторинга
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 веб-интерфейсе KUMA
Импорт информации об активах и уязвимостях активов из Kaspersky Security Center
Импорт информации об активах из MaxPatrol
Импорт данных из отчетов MaxPatrol
Импорт данных об активах из MaxPatrol VM
Параметры конфигурационного файла kuma-ptvm-config.yaml
Импорт информации об активах из KICS for Networks
Примеры сравнения полей активов при импорте
Назначение активу категории
Изменение параметров активов
Архивирование активов
Удаление активов
Массовое удаление активов
Обновление программ 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
Обнаружение неизвестных активов
Настраиваемые поля активов
Активы критической информационной инфраструктуры
Интеграция с другими решениями
Интеграция с Kaspersky Security Center
Настройка параметров интеграции с Kaspersky Security Center
Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center
Удаление тенанта из списка тенантов для интеграции с Kaspersky Security Center
Создание подключения к Kaspersky Security Center
Изменение подключения к Kaspersky Security Center
Удаление подключения к Kaspersky Security Center
Импорт событий из базы Kaspersky Security Center
Интеграция с Kaspersky Endpoint Detection and Response
Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kafka
Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kata/edr
Настройка отображения ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации о событии KUMA
Интеграция с Kaspersky CyberTrace
Интеграция поиска по индикаторам CyberTrace
Настройка CyberTrace для приема и обработки запросов
Создание правил обогащения событий
Интеграция интерфейса CyberTrace
Настройка обогащения событий и ретроспективного сканирования
Интеграция с Kaspersky Threat Intelligence Portal
Инициализация интеграции с Kaspersky Threat Intelligence Portal
Запрос данных от Kaspersky Threat Intelligence Portal
Просмотр данных от Kaspersky Threat Intelligence Portal
Обновление данных от Kaspersky Threat Intelligence Portal
Интеграция с R-Vision Security Orchestration, Automation and Response
Настройка интеграции в KUMA
Настройка интеграции в R-Vision SOAR
Добавление полей инцидента ALERT_ID и ALERT_URL
Создание коллектора в R-Vision SOAR
Создание коннектора в R-Vision SOAR
Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision SOAR
Работа с алертами с помощью R-Vision SOAR
Интеграция с Active Directory, Active Directory Federation Services и FreeIPA
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 частоты обновления данных
Изменение срока хранения данных
Запуск задач на обновление данных об учетных записях
Удаление подключения к LDAP-серверу
Аутентификация с помощью доменных учетных записей
Включение и выключение доменной аутентификации
Настройка соединения KUMA с FreeIPA
Настройка соединения KUMA с Active Directory
Настройка соединения KUMA с Active Directory Federation Services
Настройка подключения на стороне Active Directory Federation Services
Устранение ошибки Access denied при входе в KUMA через ADFS
Интеграция с НКЦКИ
Интеграция с Security Orchestration Automation and Response Platform (SOAR)
Настройка интеграции в KUMA
Настройка интеграции в SOAR
Импорт и настройка коннектора
Настройка обработчика, расписания и рабочего процесса
Интеграция с KICS for Networks и KATA
Настройка интеграции в KICS for Networks и KATA
Настройка интеграции в KUMA
Включение и выключение интеграции с KICS for Networks или KATA
Изменение частоты обновления данных
Особенности импорта информации об активах из KICS for Networks и KATA
Изменение статуса актива KICS for Networks и KATA
Интеграция с Kaspersky Automated Security Awareness Platform
Создание токена в ASAP и получение ссылки для API-запросов
Настройка интеграции в KUMA
Просмотр данных о пользователях ASAP 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
Настройка правила реагирования для интеграции с KSMG
Интеграция с Kaspersky Managed Detection and Response
Предварительная настройка
Инициализация интеграции

Импорт информации об активах из RedCheck
Настройка получения событий Sendmail
Настройка журналирования Sendmail
Настройка передачи событий Sendmail
Управление KUMA
Вход в веб-интерфейс решения
Настройка параметров Ядра KUMA
Мониторинг сервисов
Просмотр метрик KUMA
Условия срабатывания алертов по метрикам KUMA
Работа с задачами KUMA
Просмотр таблицы задач
Настройка отображения таблицы задач
Просмотр результата выполнения задачи
Повторный запуск задачи
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
Уведомления KUMA
Журналы KUMA
Работа с геоданными
Формат геоданных
Конвертация геоданных из MaxMind и IP2Location
Импорт и экспорт геоданных
Сопоставление геоданных по умолчанию
Руководство пользователя
Ресурсы KUMA
Операции с ресурсами
Создание, переименование, перемещение и удаление папок с ресурсами
Создание, дублирование, перемещение, редактирование и удаление ресурсов
Массовое удаление ресурсов
Привязка ресурсов к сервисам
Обновление ресурсов
Настройка пользовательского источника с использованием Kaspersky Update Utility
Экспорт ресурсов
Импорт ресурсов
Поиск ресурсов
Управление тегами
Трассировка использования ресурсов
Версионирование ресурсов
Сравнение версий ресурса
Восстановление версии ресурса
Настройка срока хранения версий ресурсов

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

Нормализаторы
- Параметры парсинга событий
- Расширенная схема событий
  - 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
- Обогащение в нормализаторе
- Условия передачи данных в дополнительный нормализатор
- Поддерживаемые источники событий

Правила агрегации

Правила обогащения
- Настройка параметров обогащения коллекторов активами
- Применение правила обогащения при изменении параметров коллектора

Правила сбора и анализа данных
- Настройка планировщика для правила сбора и анализа данных

Правила корреляции
- Правило корреляции, тип standard
- Правило корреляции, тип simple
- Правило корреляции, тип operational
- Правило корреляции, тип periodical
  - Создание правила корреляции в коррелятоpe correlator-ng
  - Параметры файла correlation-rules.yaml
- 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
- Добавление временного списка исключений для корреляционного правила

Предустановленные правила корреляции
Техники и тактики MITRE ATT&CK
Добавление в корреляторе правил обогащения MITRE
Импорт списка техник MITRE ATT&CK
Привязка техник MITRE ATT&CK к правилам корреляции
Экспорт правил корреляции в MITRE ATT&CK Navigator
Конвертер правил Sigma
Подготовка правила Sigma
Поддерживаемые примеры конвертации правил Sigma
Фильтры
Активные листы
Просмотр таблицы активных листов коррелятора
Добавление активного листа
Просмотр параметров активного листа
Изменение параметров активного листа
Дублирование активного листа
Удаление активных листов
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 записей в активный лист
Экспорт записей из активного листа
Предустановленные активные листы
Прокси-серверы
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 реагирования с EDR-действиями
Настройка правил реагирования с EDR-действиями
Шаблоны уведомлений
Создание шаблона уведомления
Изменение шаблона уведомления
Удаление шаблона уведомления
Синтаксис шаблонов уведомлений
Коннекторы
Просмотр параметров коннектора
Добавление коннектора
Параметры коннекторов
Коннектор, тип internal
Коннектор, тип tcp

Коннектор, тип udp
Коннектор, тип netflow
Коннектор, тип sflow
Коннектор, тип nats-jetstream
Коннектор, тип kafka
Коннектор, тип http
Коннектор, тип sql
Коннектор, тип file
Коннектор, тип 1c-log
Коннектор, тип 1c-xml
Коннектор, тип diode
Коннектор, тип ftp
Коннектор, тип nfs
Коннектор, тип wmi
Коннектор, тип wec
Коннектор, тип etw
Коннектор, тип snmp
Коннектор, тип snmp-trap
Настройка источника SNMP-trap сообщений для Windows
Настройка и запуск служб SNMP и SNMP Trap
Настройка службы Event to Trap Translator
Коннектор, тип kata/edr
Коннектор, тип vmware
Коннектор, тип elastic
Коннектор, тип office365
Коннектор, тип dfi
Коннектор, тип universalAPI
Предустановленные коннекторы
Секреты
Правила сегментации
Создание правила сегментации
Привязка правил сегментации к правилам корреляции
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 и поиск записей контекстной таблицы
Добавление, изменение и удаление записей в контекстной таблице
Экспорт данных из контекстной таблицы
Импорт данных в контекстную таблицу
Пример расследования инцидента с помощью Kaspersky SIEM
Условия возникновения инцидента
Шаг 1. Предварительная подготовка
Шаг 2. Назначение алерта пользователю

Шаг 3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта
Шаг 4. Анализ информации об алерте
Шаг 5. Проверка на ложное срабатывание
Шаг 6. Определение критичности алерта
Шаг 7. Создание инцидента
Шаг 8. Расследование
Шаг 9. Поиск связанных активов
Шаг 10. Поиск связанных событий
Шаг 11. Запись причин инцидента
Шаг 12. Реагирование на инцидент
Шаг 13. Восстановление работоспособности активов
Шаг 14. Закрытие инцидента
Аналитика
Работа с событиями
Фильтрация и поиск событий
Выбор хранилища
Формирование SQL-запроса с помощью конструктора
Создание SQL-запроса вручную
Сохранение истории запросов
Работа с сохраненными поисковыми запросами
Фильтрация событий по периоду
Отображение списка событий при относительном и точном календарном периоде
Группировка событий
Отображение названий вместо идентификаторов
Пресеты
Ограничение сложности запросов в режиме расследования алерта
Сохранение и выбор конфигураций фильтра событий
Удаление конфигураций фильтра событий
Поддерживаемые функции ClickHouse
Просмотр информации о событии
Экспорт событий
Настройка таблицы событий
Обновление таблицы событий
Получение статистики по событиям в таблице
Просмотр информации о корреляционном событии
Формирование SQL-запроса с помощью SQL-функций KUMA
Использование набора функций enrich в SQL-запросах
Использование набора функций lookup в SQL-запросах
Отслеживание маршрута событий
Категоризация событий
Гранулярный доступ к событиям
Панели мониторинга
Создание панели мониторинга
Выбор панели мониторинга
Выбор панели мониторинга в качестве панели мониторинга по умолчанию
Изменение параметров панели мониторинга
Удаление панели мониторинга

- Включение и выключение режима ТВ
- Определение периода без изменения параметров панели мониторинга
- Предустановленные панели мониторинга
- Универсальность панелей мониторинга
- Экспорт панелей мониторинга
- Импорт панелей мониторинга

Отчеты

- 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

Виджеты

- Основные принципы работы с виджетами
- Особенности отображения данных в виджетах
- Создание виджета
- Редактирование виджета
- Удаление виджета
- Параметры виджетов
  - Виджет События
  - Виджет Активные листы
  - Виджет Контекстные таблицы
  - Пользовательский виджет Активы
  - Виджет Изображение
  - Виджет Текст
  - 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

Работа с алертами

- Настройка таблицы алертов
  - Фильтрация алертов
  - Сохранение и выбор фильтра алертов
  - Удаление фильтра алертов
- Просмотр подробной информации об алерте
- Изменение названия алертов

Настройка параметров наполнения алертов
Обработка алертов
Расследование алерта
Хранение алертов и инцидентов
Уведомления об алертах
Работа с инцидентами
О таблице инцидентов
Сохранение и выбор конфигураций фильтра инцидентов
Удаление конфигураций фильтра инцидентов
Просмотр подробной информации об инциденте
Создание инцидента
Обработка инцидентов
Изменение инцидентов
Автоматическая привязка алертов к инцидентам
Категории и типы инцидентов
Взаимодействие с НКЦКИ
Экспорт данных в НКЦКИ
Получение инцидентов от НКЦКИ
Дополнение данных об инциденте по запросу
Отправка файлов в НКЦКИ
Обмен сообщениями с сотрудниками НКЦКИ
Допустимые категории и типы инцидентов НКЦКИ
Уведомления об изменении статуса инцидента в НКЦКИ
Ретроспективная проверка
Обращение в Службу технической поддержки
REST API
Создание токена
Настройка прав доступа к API
Авторизация API-запросов
Стандартная ошибка
Операции REST API v3
Приложения
Команды для запуска и установки компонентов вручную
Проверка целостности файлов KUMA
Модель данных нормализованного события
Настройка модели данных нормализованного события из KATA EDR
Модель данных алерта
Модель данных актива
Модель данных учетной записи
События аудита KUMA
Пользователь успешно вошел в систему или не смог войти
Логин пользователя изменен
Другие данные пользователя изменены
Пользователь вышел из системы
Пароль пользователя изменен
Пользователь создан
Пользователю назначена роль

Роль пользователя отозвана

Пользователь изменил параметры набора полей для определения источников

Пользователю назначен алерт

Токен доступа пользователя изменен

Добавлен файл ключа

Приложение активировано с помощью кода активации

Резервный лицензионный ключ добавлен

Резервный лицензионный ключ удален

Срок действия лицензии продлен

Недействительный код активации

Код активации заблокирован

Код активации или файл ключа удален

Код активации или файл ключа заменен

Превышено количество EPS

Окончание срока действия лицензии и начало льготного периода

Окончание льготного периода

Добавлен код активации или файл ключа с истекшим сроком годности

Изменен набор пространств для разграничения доступа к событиям

Изменены пороговые значения для мониторинга сервисов

Изменены значения параметров Ядра KUMA

Базы GeoIP импортированы

Сервис создан

Сервис удален

Сервис перезагружен

Сервис перезапущен

Сервис запущен

Сервис сопряжен

Статус сервиса изменен

Партиция удалена пользователем

Партиция удалена автоматически по истечении срока хранения

Удаление партиции по абсолютному сроку хранения

Удаление партиции по относительному сроку хранения

Перемещение партиции в холодное хранилище

Перемещение партиции в холодное хранилище завершилось с ошибкой

Активный лист успешно очищен или операция завершилась с ошибкой

Элемент активного листа успешно изменен или операция завершилась с ошибкой

Элемент активного листа успешно удален или операция завершилась с ошибкой

Активный лист успешно импортирован или операция завершилась с ошибкой

Активный лист экспортирован

Контекстная таблица экспортирована

Контекстная таблица успешно импортирована или операция завершилась с ошибкой

Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой

Контекстная таблица успешно очищена или операция завершилась с ошибкой

Ресурс добавлен

Ресурс удален

Ресурс обновлен

Импорт ресурсов
Актив создан
Актив удален
Категория актива добавлена
Категория актива удалена
Параметры обновлены
Тенант создан
Тенант включен
Тенант выключен
Другие данные тенанта изменены
Словарь успешно обновлен на сервисе или операция завершилась ошибкой
Запись добавлена в словарь
Запись успешно удалена из словаря или операция завершилась с ошибкой
Инцидент успешно создан или операция завершилась с ошибкой
Инцидент успешно закрыт или операция завершилась с ошибкой
Пользователю назначен инцидент или операция завершилась с ошибкой
Алерт привязан к инциденту или алерт отвязан от инцидента или операция завершилась с ошибкой
Зарегистрирован алерт Metrics для сервиса или операция завершилась с ошибкой
Событие привязано к алерту или отвязано от алерта или операция завершилась с ошибкой
Реагирование в Active Directory
Создание поля расширенной схемы события
Редактирование поля расширенной схемы события
Импорт поля расширенной схемы события
Импорт нормализатора с полем расширенной схемы события
Удаление поля расширенной схемы события
Отправлен запрос в KIRA
Реагирование через KICS/KATA
Реагирование через Kaspersky Automated Security Awareness Platform
Реагирование через KEDR
Импорт техник и тактик MITRE ATT&CK
Резервное копирование Ядра KUMA и восстановление из резервной копии
Резервное копирование партиций, восстановление из резервной копии, импорт партиций из сторонней установки KUMA
Правила корреляции
Отправка тестовых событий в KUMA
Формат времени
Сопоставление полей предустановленных нормализаторов
Устаревшие ресурсы
Генерация событий для тестирования работы нормализатора
Глоссарий
SELinux (Security-Enhanced Linux)
SIEM
STARTTLS
UserPrincipalName
Агрегация
Веб-интерфейс KUMA
Кластер

- Коллектор
- Коннектор
- Корреляционное правило
- Нормализатор
- Нормализация
- Обогащение
- Отчет
- Панель мониторинга
- Парсинг
- Роль
- Сетевой порт
- Событие
- Сырое событие
- Фильтр

Информация о стороннем коде

Уведомления о товарных знаках

The MITRE Corporation Terms of Use

Известные ограничения и проблемы

Справка Kaspersky Unified Monitoring and Analysis Platform

Новые функции

- Что нового в KUMA

Аппаратные и программные требования

- Аппаратные и программные требования

Начало работы

- Архитектура решения
- Установка и удаление
- Работа с тенантами
- Мониторинг источников событий

Работа в веб-интерфейсе KUMA

- Руководство администратора
- Руководство пользователя

Дополнительные возможности

- Взаимодействие с внешними системами по API

Лицензирование

- Лицензирование KUMA

Обращение в Службу технической поддержки

- Способы получения технической поддержки

О решении

Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA, или Kaspersky SIEM, или "решение") – это решение класса SIEM, предназначенное для централизованного сбора, хранения и анализа событий информационной безопасности. Решение помогает выявлять подозрительную активность и инциденты безопасности, обеспечивает возможность визуализации накопленных данных, построения автоматизированных отчетов, а также обеспечивает аналитическую поддержку процессов мониторинга и расследования в инфраструктуре организации.

Решение построено на микросервисной архитектуре. Функциональность KUMA реализована в виде отдельных сервисов, которые можно разворачивать и настраивать независимо друг от друга. Это позволяет изменять конфигурацию решения в зависимости от особенностей инфраструктуры организации, масштабировать обработку событий и обеспечивать отказоустойчивость системы.

Доступные функциональные возможности:

Потоковая корреляция в реальном времени и корреляция по индексированным данным

Kaspersky SIEM осуществляет централизованный сбор и анализ событий информационной безопасности, корреляцию событий в реальном времени и своевременное оповещение об инцидентах, а также позволяет анализировать накопленные данные и выполнять их группировку, агрегацию, нормализацию и корреляцию с помощью правил сбора и анализа данных.

Интеграция с Kaspersky Threat Intelligence

Решение Kaspersky SIEM тесно интегрировано с портфолио сервисов Kaspersky Threat Intelligence. Интеграция с Kaspersky CyberTrace позволяет применять для проверки потоки данных об угрозах и использовать обогащенные данные для корреляции и поисковых запросов. Интеграция с Kaspersky Threat Intelligence Portal (Threat Lookup) позволяет получать доступ к контекстной информации по новым атакам, индикаторам компрометации, тактикам и техникам злоумышленников.

Панели мониторинга

Панели мониторинга предназначены для отслеживания состояния безопасности сети и представляют собой гибко настраиваемый набор виджетов, отображающих различную аналитику данных безопасности.

Сбор информации об активах и реагирование на инциденты

В Kaspersky SIEM реализован автоматический сбор инвентаризационной информации (установленное ПО, уязвимости, оборудование, владелец актива), которая может использоваться для корреляции событий ИБ с учетом контекста, а также при расследовании инцидентов. Возможность управления агентами, установленными на конечных устройствах, помогает в процессе реагирования на выявленные инциденты.

Интеграция с Kaspersky Investigation and Response Assistant (KIRA)

Kaspersky SIEM поддерживает интеграцию с Kaspersky Investigation and Response Assistant (KIRA) – LLM-инструментом для расследования и приоритизации алертов. KIRA выполняет деобфускацию вывода командной строки, формирует развернутый анализ с кратким резюме для оперативного принятия решений, снижает количество ошибок при обработке инцидентов, уменьшает требования к квалификации аналитиков первой линии и сокращает время, затрачиваемое администраторами на анализ событий.

Ретроспективное сканирование

Kaspersky SIEM позволяет анализировать не только события в реальном времени, но и применять новые правила корреляции к событиям, произошедшим ранее. Это может быть полезным для более точной настройки правил корреляции, а также для ретроспективного анализа собранных данных.

Решение не предназначено для распространения на территории США. Функциональность продукта, включая получение обновлений антивирусных сигнатур и обновлений кодовой базы, может быть недоступна при использовании программы на территории США.

Что нового

В Kaspersky Unified Monitoring and Analysis Platform версии 4.2 появились следующие возможности и доработки:

- Доступна установка сервиса Метрики на произвольном хосте. Сервис Метрики должен быть только один. При установке KUMA с нуля необходимо указать хост для установки сервиса Метрики в секции `kuma_metrics` в файле инвентаря. При обновлении KUMA до версии 4.2 необходимо указать хост, на котором установлен активный сервис Метрики, в секции `kuma_metrics` в файле инвентаря. Например, если в KUMA 4.0 сервис Метрики был установлен на хосте kuma-core.example.com, перед выполнением обновления до версии 4.2 следует указать хост kuma-core.example.com в секции `kuma_metrics` в файле инвентаря. Если вы хотите перенести сервис Метрики на другой хост, вы можете использовать установщик expand.sh и файл инвентаря expand.inventory.yml.

  При переносе Ядра KUMA в кластер Kubernetes необходимо предварительно перенести сервис Метрики на один хост с Ядром KUMA при помощи установщика expand.sh и файла инвентаря expand.inventory.yml. При переносе Ядра KUMA в кластер Kubernetes выполняется проверка наличия запущенного сервиса Метрики на этом хосте. Если сервис Метрики не найден, вернется ошибка и перенос будет прерван. При переносе Ядра KUMA в кластер Kubernetes данные метрик переносятся в кластер.

- Доступно резервное копирование партиций по расписанию, резервное копирование партиций вручную, восстановление партиций из резервной копии и импорт партиций из сторонней установки KUMA.

- Резервное копирование и восстановление Ядра KUMA теперь можно выполнить через веб-интерфейс.

- После обновления KUMA с версии 4.0 до версии 4.2 доступно обновление компонентов кластера Kubernetes.

- В дополнение к предустановленным ролям появилась возможность создания пользовательских ролей. Для пользовательских ролей можно формировать уникальные наборы прав и полномочий с указанием необходимых пользователю функциональных областей.

- Для холодного хранения данные с кластера ClickHouse теперь можно переносить в облачное хранилище S3.

- В коннекторе типа kafka для авторизации теперь используются защищенные механизмы подключения SCRAM-SHA-256 и SCRAM-SHA-512.

- Добавлен коннектор типа **universalAPI** для получения данных из произвольных REST API с поддержкой JSON, фильтрации по идентификатору и режима итераций.

- Появилась возможность запускать поисковые SQL-запросы в фоновом режиме с пониженным приоритетом и просматривать результаты после завершения выполнения.

- Под учетной записью с правами Главного администратора теперь можно просматривать активные запросы других пользователей, а также управлять ими.

- Доступно новое правило корреляции типа **periodical**, которое используется для выявления несанкционированного использования учетных записей путем обнаружения аномальной активности пользователей, которая может указывать на компрометацию учетной записи. Создание этого правила доступно только при использовании коррелятора correlator-ng.

- Добавлена возможность настройки часового пояса и формата ISO 8601 в учетной записи пользователя, а также выбора первого дня недели для всего экземпляра KUMA (доступно только пользователям с ролью Главный администратор).

- В таблице раздела **Алерты** добавлен столбец **Дополнительная информация**, в котором отображается значение поля корреляционного события, выбранного при настройке параметров наполнения алерта. Для некоторых полей автоматически отображаются связанные значения, которые выводятся вместе с основным значением в карточке алерта.

- Теперь можно привязывать ресурсы (правила корреляции, правила обогащения, правила реагирования, правила агрегирования и точки назначения) к таким сервисам, как коллекторы, корреляторы и маршрутизаторы событий. Доступные сервисы зависят от типа выбранного ресурса.

- Добавлен новый тип точек назначения **udp**, позволяющий передавать нормализованные события по протоколу UDP из коллекторов и корреляторов.

- В контекстных таблицах добавлена возможность экспорта данных в форматах CSV и TSV.

- Добавлена возможность форматирования отображения события в области деталей **Информация о событии**. С помощью кнопки **Форматировать** вы можете переключать формат отображения события между однострочным и многострочным (с отступами) форматом XML или JSON.

- С помощью коннектора типа **http** KUMA может принимать события как в несжатом, так и в сжатом виде. При поступлении событий в сжатом виде, например событий Kaspersky Endpoint Security for Windows, декомпрессия событий происходит автоматически.

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-ansible-installer-<номер сборки>.tar.gz – используется для установки KUMA без использования Kubernetes. Доступна распределенная установка с Ядром KUMA в кластере на основе алгоритма Raft.

- kuma-ansible-installer-k8s-<номер сборки>.tar.gz – используется для установки KUMA в отказоустойчивой конфигурации на базе Kubernetes.

- Файлы с информацией о версии (примечания к выпуску) на русском и английском языках.

Аппаратные и программные требования

Рекомендуемые требования к оборудованию

В этом разделе приведены требования к оборудованию для обработки различных вариантов потока событий в секунду (Events per Second, далее EPS), поступающих в KUMA.

В таблице ниже приведены аппаратные и программные требования к оборудованию для установки компонентов KUMA, исходя из представления, что кластер ClickHouse принимает только запросы INSERT. Требования к оборудованию для удовлетворения потребностей по запросам SELECT рассчитывается отдельно под конкретный профиль использования СУБД заказчика.

Рекомендуемые требования к оборудованию для хранилищ кластера ClickHouse

При расчете конфигурации кластера хранения нужно учитывать количество EPS, средний размер события и глубину хранения, а также требования к дисковой подсистеме, сетевому интерфейсу, оперативной памяти и профилю использования.

Дисковая подсистема

Основная нагрузка на ClickHouse в KUMA — это операции записи (вставки):

- События поступают в СУБД практически постоянным потоком.
- Вставки, по меркам ClickHouse, частые и мелкие.
- ClickHouse отличается высоким показателем амплификации записи (write amplification) за счет постоянных фоновых слияний частей партиций (parts).
- Часть партиции размером до 1 ГБ хранится в виде одного файла. При превышении размера в 1 ГБ для части применяется ширококолоночный формат (wide column format), где каждый столбец таблицы представлен в виде двух файлов .dat и .mrk. В этом случае для перезаписи части партиции в результате ее слияния с другой частью, требуется запись в 384 файла + fsync на каждый, что подразумевает большое количество IOPS.

ClickHouse одновременно выполняет и поисковые запросы, но их значительно меньше, чем операций записи. С учетом характера нагрузки мы рекомендуем следующий подход к организации дисковой подсистемы:

- Использовать DAS (Direct Attached Storage) с NVME или SAS/SATA-интерфейсами, избегая решений класса SAN/NAS.
- Если узлы кластера ClickHouse развернуты в виртуальной среде, директория `/opt/kaspersky/kuma` должна быть напрямую смонтирована на дисковый массив. Не следует использовать виртуальные диски.
- Использовать SSD (SATA/NVME). Любые SSD серверного класса обеспечат большую производительность, чем HDD (даже 15 000 RPM). Для SSD следует использовать RAID-10 или RAID-0 (если используется репликация в ClickHouse).

  Если использовать SSD невозможно, следует применять HDD 15 000 RPM, SAS, объединенные в RAID-10.

  Допускается гибридный вариант, когда горячие данные (например, за последний месяц) хранятся на SSD, а холодные данные — на HDD. Таким образом, операции записи всегда будут адресованы SSD-массивам.

  При использовании гибридного варианта SSD и HDD нужно учитывать, что программный RAID-массив (madm) всегда будет демонстрировать более высокую производительность и гибкость, чем аппаратный RAID-контроллер. При использовании RAID-0 или RAID-10 важно, чтобы размер полосы (stripe size) был равен 1 МБ. Часто в аппаратных RAID-контроллерах размер полосы по умолчанию составляет 64 КБ, а максимально доступное значение — 256–512 КБ. Для RAID-10 наиболее оптимальным для записи является near-layout, а для чтения — far-layout.
- Рекомендуемая файловая система — EXT4. Если использовать EXT4 невозможно, допустимо использовать файловую систему XFS. Для любой из этих файловых систем рекомендуется включить опцию монтирования noatime.

Сетевой интерфейс

Рекомендации для сетевого интерфейса:

1. На каждом узле кластера должен быть установлен и скоммутирован сетевой интерфейс с пропускной способностью не менее 10 Гбит/с. С учетом амплификации записи и репликации наиболее подходящим решением будет 25 Гбит/с.

2. При необходимости процессы репликации могут использовать обособленный сетевой интерфейс, который не обрабатывает трафик, связанный со вставками и поисковыми запросами.

Оперативная память

ClickHouse рекомендует использовать соотношение объема оперативной памяти к объему данных, хранящихся на узле, равное 1:100.

Однако при расчете требований к оперативной памяти следует учитывать не только общий объем хранимых данных, но и объем данных, который в среднем обрабатывается при выполнении запросов. Например, если средний запрос предполагает сканирование партиций суммарным объемом 10 ТБ, рекомендуется предусмотреть не менее 100 ГБ оперативной памяти. Приведенное соотношение является общей рекомендацией и рассчитано на выполнение широких аналитических запросов. Фактические требования к оперативной памяти зависят от характера запросов, объема обрабатываемых данных и конфигурации системы.

Наличие свободной памяти на сервере положительно влияет на производительность поисковых запросов по наиболее свежим событиям, так как содержимое файлов партиций будет продублировано в кеш операционной системы и будет считываться из оперативной памяти, а не с диска.

Профиль использования

Требования к оборудованию рассчитаны на поглощение СУБД потока в n EPS при нахождении СУБД в покое (поисковые запросы не выполняются, только операции записи). На этапе внедрения KUMA не всегда удается точно определить, какие поисковые и аналитические запросы будут выполняться в системе, интенсивность, конкурентность и глубину поисковых запросов, а также фактическую производительность узлов кластера.

Таким образом, масштабирование кластера ClickHouse в процессе эксплуатации KUMA является стандартным сценарием. Если в результате увеличения потока EPS или увеличения интенсивности либо ресурсоемкости поисковых запросов кластер перестает справляться с нагрузкой, следует либо добавить шарды (горизонтальное масштабирование), либо усовершенствовать дисковые подсистемы, CPU или оперативную память на узлах кластера.

Конфигурацию оборудования необходимо подбирать исходя из профиля нагрузки системы. Допустимо использовать конфигурацию типа "All-in-one" при обрабатываемом потоке событий до 10 000 EPS и при использовании графических панелей, поставляемых с системой.

KUMA поддерживает работу с процессорами Intel или AMD с поддержкой набора инструкций SSE 4.2 и набора инструкций AVX.

	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Требования к Ядру KUMA	–	–	Одно устройство. Характеристики устройства: • от 12 потоков или vCPU; • от 12 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 53 Мбит/с.	Одно устройство. Характеристики устройства: • от 16 потоков или vCPU; • от 24 ГБ оперативной памяти; • от 1 ТБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 134 Мбит/с.
Требования к коллектору	–	–	Одно устройство. Характеристики устройства: • от 16 потоков или vCPU; • от 24 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 53 Мбит/с.	Два устройства. Характеристики каждого устройства: • от 16 потоков или vCPU; • от 24 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 134 Мбит/с.
Требования к коррелятору	–	–	Одно устройство. Характеристики устройства: • от 16 потоков или vCPU; • от 32 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 53 Мбит/с.	Одно устройство. Характеристики устройства: • от 16 потоков или vCPU; • от 32 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 134 Мбит/с.
Требования к маршрутизатору событий	–	Процессор: 3 ядра. Оперативная память: 240 МБ.	Процессор: 6 ядер. Оперативная память: 250 МБ.	Процессор: 9 ядер. Оперативная память: 7000 МБ.
Требования к киперу	–	–	Три устройства. Характеристики каждого устройства: • от 6 потоков или vCPU; • от 12 ГБ оперативной памяти; • от 100 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 53 Мбит/с.	Три устройства. Характеристики каждого устройства: • от 6 потоков или vCPU; • от 12 ГБ оперативной памяти; • от 100 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 134 Мбит/с.

	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Требования к хранилищу	–	–	Два устройства. Характеристики каждого устройства: • от 24 потоков или vCPU; • от 64 ГБ оперативной памяти; • от 16.5 ТБ в каталоге /opt; • тип хранилища данных – SSD*. Рекомендуемая скорость передачи данных между узлами ClickHouse должна быть не менее 10 Гбит/с, если поток событий равен или превышает 20 000 EPS.	Четыре устройства. Характеристики каждого устройства: • от 24 потоков или vCPU; • от 64 ГБ оперативной памяти; • от 41.3 ТБ в каталоге /opt; • тип хранилища данных – SSD*. Рекомендуемая скорость передачи данных между узлами ClickHouse должна быть не менее 10 Гбит/с, если поток событий равен или превышает 20 000 EPS.
Операционные системы	• Ubuntu 22.04 LTS. • Ubuntu 24.04 LTS. • Oracle Linux 8.x. • Oracle Linux 9.x. • Astra Linux Special Edition РУСБ.10015-01 1.7.x (начиная с версии 2021-1126SE17 оперативное обновление 1.7.1). • Astra Linux Special Edition РУСБ.10015-01 1.8.x (начиная с версии 2025-0114SE18MD срочное оперативное обновление 1.8.1.UU.2). • РЕД ОС 7.3.4. • РЕД ОС 8. • МосОС 15.5.			
Криптонаборы TLS	Поддерживается протокол TLS версии 1.2 и 1.3. Интеграция с сервером, не поддерживающим версии и криптонаборы TLS, которые требует KUMA, невозможна. Поддерживаемые криптонаборы TLS 1.2: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256. • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. Поддерживаемые криптонаборы TLS 1.3: • TLS_AES_128_GCM_SHA256. • TLS_AES_256_GCM_SHA384. • TLS_CHACHA20_POLY1305_SHA256.			

Рекомендуемые конфигурации при разных уровнях нагрузки

В таблице ниже описаны состав конфигураций и рекомендуемые ресурсы для компонентов KUMA в зависимости от уровня EPS, включая требования к хранилищу и рекомендации по масштабированию.

Рекомендуемые конфигурации оборудования и потребление ресурсов KUMA в зависимости от EPS

Параметр	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Тип установки	Установка на одном сервере.	Установка на одном сервере.	Распределенная установка на нескольких серверах.	Распределенная установка на нескольких серверах.
Количество серверов и их назначение	Один сервер, на котором размещаются все компоненты системы.	Один сервер, на котором размещаются все компоненты системы.	Один сервер для Ядра KUMA. Один сервер для коллектора. Один сервер для коррелятора. Три выделенных сервера с ролью кипера. Два сервера для хранилища.	Один сервер для Ядра KUMA. Два сервера для коллектора. Один сервер для коррелятора. Три выделенных сервера с ролью кипера. Четыре сервера для хранилища.

Параметр	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Аппаратные характеристики серверов	От 16 потоков или 16 vCPU. От 32 ГБ оперативной памяти. От 500 ГБ в директории /opt. Тип хранилища данных – SSD. Скорость передачи данных – от 100 Мбит/с.	От 24 потоков или 24 vCPU. От 64 ГБ оперативной памяти. От 500 ГБ в директории /opt. Тип хранилища данных – SSD. Скорость передачи данных – от 100 Мбит/с.	См. характеристики для компонентов KUMA в таблице выше. Для хранилища требуются быстрые SSD, высокая IOPS, пропускная способность сети от 1 Гбит/с.	Те же характеристики, что и для 20 000 EPS, но с удвоенным количеством коллекторов и серверов хранилища. Повышенные требования к сетевому взаимодействию между всеми узлами: рекомендуется пропускная способность сети от 1 Гбит/с.
Конфигурация хранилища (ClickHouse)	Один шард, одна реплика. Дисковый буфер включен.	Один шард, одна реплика. Дисковый буфер включен.	Два шарда, по две реплики в каждом. При отсутствии требований отказоустойчивости допускается один сервер с одной репликой на каждый шард.	Два шарда, по две реплики в каждом. При отсутствии требований отказоустойчивости допускается два сервера с одной репликой на каждый шард.

Дополнительные рекомендации по выбору и масштабированию конфигурации:

- Для компонента Ядра KUMA при наличии более 50 000 активов рекомендуется увеличить выделенные ресурсы: на каждые дополнительные 50 000 активов следует добавить 2 потока (или 2 vCPU) и 4 ГБ оперативной памяти. Если система управляет более чем 100 сервисами, необходимо учитывать дополнительную нагрузку: на каждые 100 сервисов рекомендуется также увеличивать вычислительные ресурсы Ядра KUMA на 2 потока (или 2 vCPU).

- В случаях активного взаимодействия пользователей с системой, включая регулярное построение отчетов, работу с панелями мониторинга и выполнение пользовательских SQL-запросов, необходимо предусмотреть дополнительное масштабирование как для Ядра KUMA, так и для хранилища, поскольку такая активность существенно увеличивает нагрузку на оба компонента.

- При выборе дисковой подсистемы для хранилища (ClickHouse) следует использовать только SSD-накопители. Исключение возможно, если не планируется выполнение агрегационных SQL-запросов с глубиной более 24 часов. В этом случае допускается использование HDD с характеристиками не ниже 15 000 RPM, интерфейс SAS, объединенные в RAID-10.

- При размещении компонентов в HDFS допустимо использовать HDD независимо от характера запросов.

- Экспорт событий осуществляется через временные файлы, которые сохраняются в директории /opt/kaspersky/kuma/core/tmp/. Эти файлы автоматически удаляются через 10 суток. Если вы планируете экспортировать большой объем событий, необходимо выделить дополнительное место.

Работа в виртуальных средах

Поддерживается установка KUMA в следующих виртуальных средах:

- VMware 6.5 и выше.

- Hyper-V для Windows Server 2012 R2 и выше.

- QEMU-KVM 4.2 и выше.

- ПК СВ "Брест" РДЦП.10001-02.

- Basis Dynamix Enterprise 4.6.

Работа в облачных средах

Поддерживается работа в облачной инфраструктуре. Система может быть установлена на виртуальные машины по модели IaaS (инфраструктура как сервис).

Для работы в облачной инфраструктуре мы рекомендуем использовать конфигурации "Установка на одном сервере" для 3 000 EPS и 10 000 EPS. Виртуальные машины должны удовлетворять аппаратным и программным требованиям, предъявляемым к обычной установке.

При выборе дисковой подсистемы сервера, следует ориентироваться на параметр "количество операций ввода/вывода (IOPS)". Рекомендуемое минимальное значение 1000 IOPS.

Рекомендации для сервиса Коллектор

Следует учитывать, что для эффективной обработки событий количество ядер процессора важнее, чем их частота. Например, восемь ядер процессора со средней частотой будут эффективнее справляться с обработкой событий, чем четыре ядра с высокой частотой.

Также необходимо иметь в виду, что количество потребляемой коллектором оперативной памяти зависит от настроенных методов обогащения (DNS, учетные записи, активы, обогащение данными из Kaspersky CyberTrace) и использования агрегации (на потребление оперативной памяти влияет параметр окна агрегации данных, количество полей, по которым выполняется агрегация данных, объем данных в агрегируемых полях). Показатели использования KUMA вычислительных ресурсов зависят от типа анализируемых событий и от эффективности нормализатора.

Например, при потоке событий 1000 EPS и выключенном обогащении событий (обогащение событий выключено, агрегация событий выключена, 5000 учетных записей, 5000 активов в тенанте) одному коллектору требуются следующие ресурсы:

- 1 процессорное ядро или 1 виртуальный процессор;
- 512 МБ оперативной памяти;
- 1 ГБ дискового пространства (без учета кеша событий).

Например, для 5 коллекторов, которые не выполняют обогащение событий потребуется выделить следующие ресурсы: 5 процессорных ядер, 2,5 ГБ оперативной памяти и 5 ГБ свободного дискового пространства.

Рекомендации для серверов хранилищ

Для подключения системы хранения данных (далее СХД) к серверам хранилища следует использовать высокоскоростные протоколы, например Fibre Channel или iSCSI 10G. Для подключения СХД не рекомендуется использовать протоколы прикладного уровня, такие как NFS и SMB.

На серверах кластера ClickHouse рекомендуется использовать файловую систему ext4.

При использовании RAID-массивов рекомендуется использовать RAID 0 для достижения высокой производительности, а RAID 10 для обеспечения высокой производительности и отказоустойчивости.

Для обеспечения отказоустойчивости и быстродействия подсистемы хранения данных мы рекомендуем разворачивать все узлы ClickHouse исключительно на разных дисковых массивах.

Если вы используете виртуализированную инфраструктуру для размещения компонентов системы, мы рекомендуем разворачивать узлы кластера ClickHouse на различных гипервизорах. При этом необходимо ограничить возможность работы двух виртуальных машин с ClickHouse на одном гипервизоре.

Для высоконагруженных инсталляций KUMA рекомендуется устанавливать ClickHouse на аппаратных серверах.

Рекомендации для сервиса Метрики

Сервис Метрики обеспечивает мониторинг работы KUMA (раздел **Метрики**) и мониторинг потоков событий от источников (раздел **Состояние источников**).

На требования к вычислительной мощности сервера для сервиса Метрики влияет множество параметров, включая:

- Общее количество созданных сервисов KUMA.
- Параметры сервиса мониторинга источников событий.

Конфигурацию оборудования для сервера, на котором установлен сервис Метрики, необходимо подбирать исходя из профиля нагрузки системы.

Рекомендуемые требования к оборудованию для сервиса Метрики

Масштабирование решения в зависимости от количества сервисов

Требования к оборудованию сервера для сервиса Метрики в зависимости от количества сервисов в экземпляре KUMA приведены в таблице ниже. Расчет проводился для потока событий 20 000 EPS. Значения количества процессоров и объема ОЗУ в таблице округлены в большую сторону до целого значения.

Результаты в таблице были получены при следующих параметрах:

- Параметры обнаружения источников: по умолчанию.
- Параметры политик мониторинга:
  - **Тип**: byCount.
  - **Нижний порог**: 10.
  - **Верхний порог**: 1000.

- **Период подсчета**: 10 минут.
- **Интервал оценки**: 5 минут.

Масштабирование решения в зависимости от числа сервисов

Число сервисов	Число процессоров (рекомендуется)	ОЗУ (ГБ) (рекомендуется)
50	1	3
100	1	3
500	1	4

Из таблицы следует, что рост числа сервисов в экземпляре KUMA повышает требования к оборудованию незначительно.

Масштабирование решения в зависимости от состояния источников событий

На требования к оборудованию (процессорам, оперативной памяти и дисковому пространству) влияют следующие параметры, отображаемые или заданные в разделах **Метрики** и **Состояние источников**:

- Параметры определения источников.

  На требования к оборудованию влияют параметры, заданные для определения источников: количество полей и их свойства. Если вы увеличите количество полей или укажете поля, которые содержат большое количество уникальных значений, это может привести к тому, что KUMA определит большое количество источников событий. Как следствие, увеличение количества источников событий увеличивает требования к оборудованию.

  Например, набор полей `DeviceProduct, DeviceHostName, DeviceAddress` определит в качестве источника межсетевой экран `Firewall, fw-1.example.com, 192.0.2.1`. Если же вы зададите набор полей `DeviceProduct, DeviceHostName, DeviceAddress, Name`, KUMA определит гораздо большее количество источников событий:

  - `Firewall, fw-1.example.com, 192.0.2.1, DNS`
  - `Firewall, fw-1.example.com, 192.0.2.1, IPS`
  - `Firewall, fw-1.example.com, 192.0.2.1, TRAFFIC`
  - `Firewall, fw-1.example.com, 192.0.2.1, TREAT`

  Следует учесть, что заметное влияние на требования к оборудованию начинается при количестве источников событий, превышающем 100 000.

- Количество источников событий, которым назначены политики мониторинга, а также период подсчета данных и интервал оценки.

  KUMA получает и записывает информацию о потоке данных с каждого источника событий, которому назначена политика мониторинга, с периодичностью, указанной в политике.

- Количество политик мониторинга, назначенных каждому из источников событий.
- Средний размер точки данных (значение метрики **Bytes per point**).

С помощью значения метрики **Bytes per point** (bpp) сервиса Метрики вы можете вычислить объем дискового пространства, необходимого для хранения метрик. Для этого вы можете использовать формулу:

```
hdd_sizing = ROUNDUP (bpp * (retention_sec/interval_sec) * EPS * 1,1)
```

где:

- `hdd_sizing` – требуемый объем дискового пространства;
- `ROUNDUP` – функция округления в большую сторону;
- `bpp` – значение метрики **Bytes per point**;
- `retention_sec` – срок хранения метрик в секундах;
- `interval_sec` – интервал получения информации, равен 15 секундам;
- `EPS` – среднее значение EPS по источникам, примерно равно значению метрики **Processing EPS** на коллекторе;
- 1,1 – корректирующий коэффициент, добавляющий 10% к расчетному значению дискового пространства.

- Поток событий, обрабатываемых всеми коллекторами KUMA.

  Требования к оборудованию при масштабировании решения по числу источников событий и политик мониторинга в экземпляре KUMA приведены в таблице ниже.

  Из данных таблицы следует, что требования к оборудованию существенно повышаются при большом количестве источников событий и большом количестве политик мониторинга, назначенных источникам событий. Эти данные приведены в нижней части таблицы.

  Результаты в таблице были получены при следующих параметрах:

  - Параметры обнаружения источников: по умолчанию.
  - Параметры политик мониторинга:
    - **Тип**: byCount.
    - **Нижний порог**: 10.
    - **Верхний порог**: 1000.
    - **Период подсчета**: 10 минут.
    - **Интервал оценки**: 5 минут.

Масштабирование решения в зависимости от числа источников событий и политик мониторинга

Число источников событий	Число источников событий, отслеживаемых политиками мониторинга	EPS	Число политик мониторинга на одном источнике	Число процессоров (рекомендуется)	ОЗУ (ГБ) (рекомендуется)	Дисковое пространство (ГБ) в расчете на срок хранения метрик 30 дней
10 000	0	25 000	0	1	2	13
25 000	0	25 000	0	1	2	13

Число источников событий	Число источников событий, отслеживаемых политиками мониторинга	EPS	Число политик мониторинга на одном источнике	Число процессоров (рекомендуется)	ОЗУ (ГБ) (рекомендуется)	Дисковое пространство (ГБ) в расчете на срок хранения метрик 30 дней
50 000	0	25 000	0	1	3	13
100 000	0	25 000	0	1	3	14
250 000	0	25 000	0	1	3	13
500 000	0	25 000	0	1	5	13
1 000 000	0	25 000	0	1	7	11
10 000	2000	5000	1	1	3	4
10 000	5000	5000	1	1	3	5
10 000	2000	10 000	1	1	3	8
10 000	2000	10 000	2	1	3	10
10 000	5000	10 000	1	1	3	9
10 000	5000	25 000	1	1	3	24
10 000	10 000	5000	1	1	4	5
10 000	10 000	5000	2	1	5	5
50 000	10 000	5000	1	1	4	4
50 000	10 000	10 000	1	1	5	7
50 000	25 000	25 000	1	1	6	20
100 000	20 000	5000	1	1	6	4
100 000	20 000	10 000	1	1	6	8
100 000	100 000	5000	1	4	19	5
250 000	50 000	10 000	1	3	12	7
100 000	100 000	5000	2	6	29	5
250 000	250 000	5000	1	10	40	4
250 000	250 000	5000	2	17	68	5

Требования к устройствам для установки агентов

Для передачи данных в коллектор KUMA на устройствах сетевой инфраструктуры требуется установить агенты. Требования к устройствам приведены в таблице ниже.

	Устройства с ОС Windows	Устройства с ОС Linux
Процессор	Одноядерный, 1.4 ГГц или выше.	Одноядерный, 1.4 ГГц или выше.
ОЗУ	512 МБ	512 МБ

	Устройства с ОС Windows	Устройства с ОС Linux
Свободное дисковое пространство	1 ГБ	1 ГБ
Операционные системы	• Microsoft® Windows® 2012. Microsoft Windows 2012 поддерживается ограниченно. • Microsoft Windows Server 2012 R2. Microsoft Windows 2012 R2 поддерживается ограниченно. • Microsoft Windows Server 2016. • Microsoft Windows Server 2019. • Microsoft Windows Server 2022. • Microsoft Windows Server 2025. • Microsoft Windows 10. • Microsoft Windows 11.	• Oracle® Linux 8.x. • Oracle Linux 9.x. • Alma Linux 9.5. • Astra Linux Special Edition РУСБ.10015-01 1.7.x (начиная с версии 2021-1126SE17 оперативное обновление 1.7.1) с установленной библиотекой glibc 2.28 (Debian GLIBC 2.28-10+deb10u4+ci202407161455+astra12). • Astra Linux Special Edition РУСБ.10015-01 1.8.x (начиная с версии 2025-0114SE18MD срочное оперативное обновление 1.8.1.UU.2) с установленной библиотекой glibc 2.36 (Debian GLIBC 2.36-9+deb12u7+ci202405171200+astra5). • CentOS Linux release 8.2.2004 (Core) с установленной библиотекой glibc 2.28 (GNU libc). • CentOS Linux release 7.7.1908 (Core) с установленной библиотекой glibc 2.17 (GNU libc). • Debian 12 с установленной библиотекой glibc 2.36 (Debian GLIBC 2.36-9+deb12u7). • Red Hat Enterprise Linux 9.5 (Plow) с установленной библиотекой glibc 2.34 (GNU libc). • Red OS 8. • Rocky Linux 9.3 (Blue Onyx) с установленной библиотекой glibc 2.34 (GNU libc). • Rocky Linux 9.5. • SuSE 15.6. • Ubuntu 24.04.2 LTS с установленной библиотекой glibc 2.39 (Ubuntu GLIBC 2.39-0ubuntu8.4). • Ubuntu 22.04.4 LTS с установленной библиотекой glibc 2.35 (Ubuntu GLIBC 2.35-0ubuntu3.8). • МосОС 15.5.

Требования к устройствам для установки агентов KUMA с коннекторами WEC, ETW и WMI

Агенты KUMA, установленные на устройствах с операционной системой Windows, могут использовать различные типы коннекторов для получения событий: WEC (Windows Event Collector), ETW (Event Tracing for Windows) и WMI (Windows Management Instrumentation). Производительность агентов и их влияние на систему зависят от ограничений Windows, а также от количества и типа обрабатываемых событий (см.таблицу ниже).

Требования к агентам по типам коннектора

Тип коннектора	Максимальная производительность (EPS)	Ограничения со стороны Windows	Ограничения со стороны KUMA	Рекомендуемая конфигурация агента	Загрузка процессора и ОЗУ
WEC	До 2500 событий в секунду	При записи в системные журналы (Application, System, Hardware Events) Windows ограничивает скорость записи примерно 2500 событиями в секунду. При одновременной записи в несколько журналов производительность снижается: до 1100 EPS при 2 журналах, до 800 EPS при 3 журналах, до 500 EPS при 4 журналах.	Агент может обрабатывать события в диапазоне 1500–2500 EPS без задержек.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,18 (что эквивалентно примерно 0,28% от общей производительности системы). Использование ОЗУ – до 209 МБ.
ETW	До 700 событий в секунду	Поддерживается только один системный журнал: **Microsoft → Windows → DNS-Server**. Операционная система Windows не позволяет записывать более 700 событий в секунду в этот журнал.	Ограничений на стороне KUMA не выявлено, однако при EPS выше 700 агент не получает данные из-за ограничений Windows.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,267 (что эквивалентно примерно 0,42% от общей производительности системы). Использование ОЗУ – до 186 МБ.
WMI	До 5000 событий в секунду	Обойти ограничения Windows можно за счет подключения нескольких устройств. Каждое дополнительное устройство увеличивает общий объем событий на 1000–1500 EPS.	При достижении отметки 5000 EPS агент начинает обрабатывать события с задержкой.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,61 (что эквивалентно примерно 0,95% от общей производительности системы). Использование ОЗУ – до 311 МБ.

Аппаратные требования к агентам KUMA на устройствах Linux в зависимости от размера потока событий

Агенты KUMA, установленные на устройствах с операционной системой Linux, могут использовать различные типы транспортов. Аппаратные требования к агентам KUMA зависят от типа используемого транспорта и от потока событий (EPS) (см.таблицу ниже).

Требования к агентам на устройствах Linux в зависимости от потока событий

Тип транспорта	10 000 EPS	20 000 EPS	60 000 EPS	100 000 EPS
HTTP	Процессор: 3 ядра. Оперативная память: 160 МБ.	Процессор: 5 ядер. Оперативная память: 160 МБ.	Процессор: 6 ядер. Оперативная память: 260 МБ.	Процессор: 6 ядер. Оперативная память: 300 МБ.

Требования к устройствам для работы с сервисом AI-рейтинг и статус активов

Процессор: 2 ядра по 2,7 ГГц.

ОЗУ: 8 ГБ.

Тип накопителя: SSD или HDD.

Свободное дисковое пространство: 10 ГБ для самого сервиса и место под ОС.

Требования к клиентским устройствам для работы с веб-интерфейсом KUMA

Процессор:

- 32-разрядный Intel® Core™ i3 8-го поколения.
- 32-разрядный AMD Ryzen 3.

ОЗУ: 8 ГБ.

Поддерживаемые браузеры:

- Google™ Chrome™ 110 и выше.
- Mozilla™ Firefox™ 115 и выше.

Требования к устройствам для установки KUMA в Kubernetes

Кластер Kubernetes для развертывания KUMA в отказоустойчивом варианте включает в минимальной конфигурации:

- 1 узел балансировщика – не входит в кластер;
- 3 узла-контроллера;
- 2 рабочих узла.

Минимальные аппаратные требования к устройствам для установки KUMA в Kubernetes представлены в таблице ниже.

Минимальные аппаратные требования к устройствам для установки KUMA в Kubernetes

	Балансировщик	Контроллер	Рабочий узел
Процессор	1 ядро с 2 потоками или 2 vCPU.	1 ядро с 2 потоками или 2 vCPU.	12 потоков или 12 vCPU.
ОЗУ	От 2 ГБ	От 2 ГБ	От 24 ГБ
Свободное дисковое пространство	От 30 ГБ	От 30 ГБ	Для новых экземпляров KUMA: не менее 600 ГБ свободного дискового пространства в директории /opt/. Для существующих экземпляров KUMA: при ранее выделенном объеме 1 ТБ и более в директории /opt/ уменьшение дискового пространства не рекомендуется без предварительной консультации со Службой технической поддержки. От 32 ГБ в директории /var/lib/
Пропускная способность сети	10 Гбит/с	10 Гбит/с	10 Гбит/с

Интерфейс KUMA

Работа с решением осуществляется через веб-интерфейс.

Окно веб-интерфейса решения содержит следующие элементы:

- разделы в левой части окна веб-интерфейса решения;
- вкладки в верхней части окна веб-интерфейса решения для некоторых разделов решения;
- рабочую область в нижней части окна веб-интерфейса решения.

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на вкладках окна веб-интерфейса решения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Во время работы с веб-интерфейсом решения вы можете выполнять следующие действия с помощью горячих клавиш:

- во всех разделах: закрывать окно, открывающееся в правой боковой панели – **`Esc`**;
- в разделе **События**:
  - переключаться между событиями в правой боковой панели – ↑ и ↓;
  - запускать поиск (при фокусе на поле запроса) – **`Ctrl/Command`** + **`Enter`**;
  - сохранять поисковый запрос – **`Ctrl/Command`** + **`S`**.

Совместимость с другими программами

Kaspersky Endpoint Security для Linux

При установке на одном сервере компонентов KUMA и программы Kaspersky Endpoint Security для Linux каталог report.db может достигать больших размеров и занимать все дисковое пространство. Кроме того, Kaspersky Endpoint Security для Linux по умолчанию сканирует все файлы KUMA, включая служебные, что может влиять на производительность. Чтобы избежать этих проблем, выполните следующие действия:

- Обновите программу Kaspersky Endpoint Security для Linux до версии 12.0 или выше.
- Мы не рекомендуем включать сетевые компоненты Kaspersky Endpoint Security для Linux.

  Подробнее о рекомендуемых настройках при совместной работе с KUMA см. в онлайн-справке Kaspersky Endpoint Security для Linux.

- Добавьте в общие исключения и в исключения для проверки по требованию следующие директории:

  a. На сервере Ядра KUMA:

  - /opt/kaspersky/kuma/metrics/ - папка с данными сервиса Метрики.

  b. На сервере хранилища:

  - /opt/kaspersky/kuma/clickhouse/ - папка ClickHouse.
  - /opt/kaspersky/kuma/storage/<идентификатор хранилища>/buffers/ - папка с буферами хранилища.

  c. На сервере коррелятора:

  - /opt/kaspersky/kuma/correlator/<идентификатор коррелятора>/data/ - папки со словарями.
  - /opt/kaspersky/kuma/correlator/<идентификатор коррелятора>/lists - папки с активными листами.
  - /opt/kaspersky/kuma/correlator/<идентификатор коррелятора>/ctxtables - папки с контекстными таблицами.
  - /opt/kaspersky/kuma/correlator/<идентификатор коррелятора>/buffers - папка с буферами.

  d. На сервере коллекторов:

  - /opt/kaspersky/kuma/collector/<идентификатор коллектора>/buffets - папка с буферами.
  - /opt/kaspersky/kuma/collector/<идентификатор коллектора>/data/ - папка со словарями.

  e. Папки с журналами для каждого сервиса.

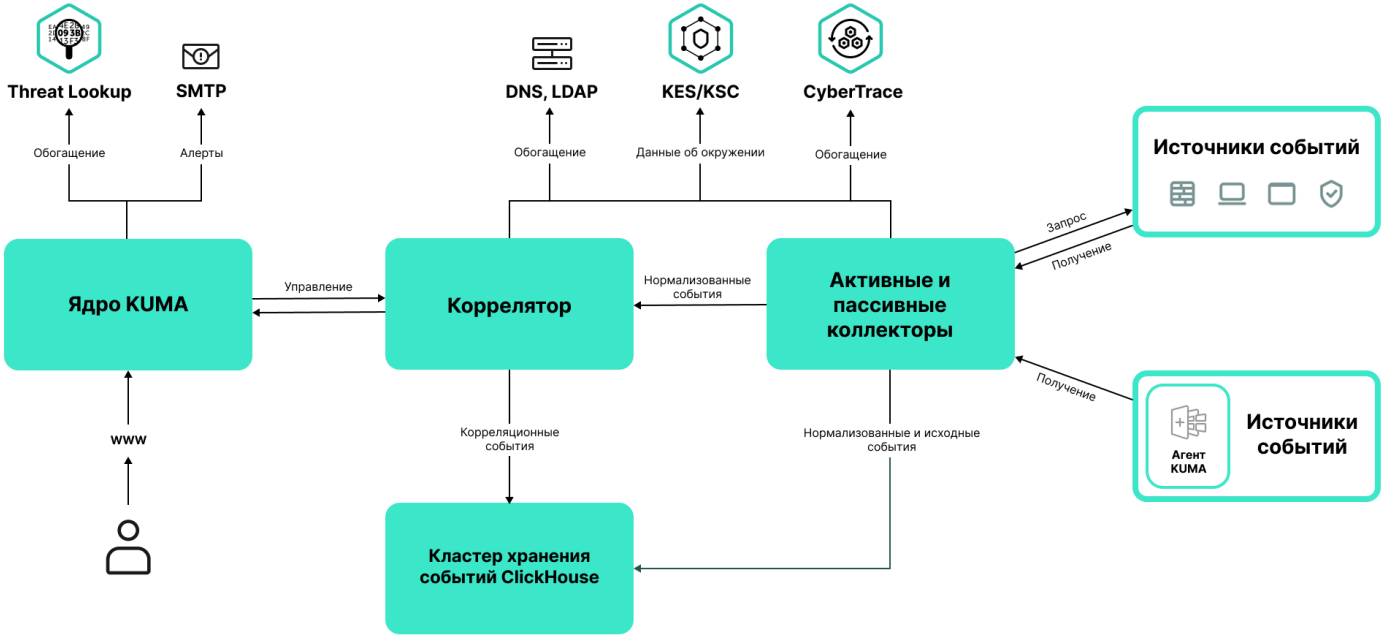
Подробнее об исключениях из проверки см. в онлайн-справке Kaspersky Endpoint Security для Linux.

Архитектура решения

Стандартная установка решения включает следующие компоненты:

- *Ядро*, включающее графический интерфейс для мониторинга и управления настройками компонентов системы.
- *Агенты*, которые используются для пересылки сырых событий с серверов и рабочих станций в точки назначения KUMA.
- Один или несколько *коллекторов*, которые получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию.
- *Маршрутизаторы событий*, которые принимают события от коллекторов и с учетом настроенных фильтров направляют события в заданных точки назначения. Таким образом, эти сервисы используются для распределения нагрузки на каналы связи.
- *Коррелятор*, который анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает алерты в соответствии с правилами корреляции.
- *Хранилище*, в котором содержатся нормализованные события и зарегистрированные алерты.

События передаются между компонентами по надежным транспортным протоколам (при желании с шифрованием). Вы можете настроить балансировку нагрузки для ее распределения между экземплярами сервисов, а также включить автоматическое переключение на резервный компонент в случае недоступности основного. Если недоступны все компоненты, события сохраняются в буфере жесткого диска и передаются позже. Размер буфера в файловой системе для временного хранения событий можно менять.



Архитектура KUMA

Ядро

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

Ядро позволяет выполнять следующие задачи:

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

Коллектор

Коллектор – это компонент решения, 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.

   В решении доступны следующие типы коннекторов:

   - tcp;
   - udp;
   - netflow;
   - sflow;
   - nats-jetstream;
   - kafka;

- kata/edr;
- http;
- sql;
- file;
- 1c-xml;
- 1c-log;
- diode;
- ftp;
- nfs;
- vmware;
- wmi;
- wec;
- snmp-trap;
- 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.

   В решении доступны следующие нормализаторы:

   - JSON;
   - CEF;
   - Regexp;
   - Syslog (как для RFC3164 и RFC5424);
   - CSV;
   - Ключ-значение;
   - XML;
   - NetFlow (единый нормализатор для NetFlow v5, NetFlow v9 и IPFIX);
   - NetFlow v5;
   - NetFlow v9;

- SQL;
- IPFIX (v10).

3. **Фильтрация нормализованных событий**

   Вы можете настроить фильтры, которые позволяют отобрать события, удовлетворяющие заданным условиям, чтобы передать их в обработку.

4. **Обогащение и преобразование нормализованных событий**

   Правила обогащения позволяют дополнить содержащуюся в событии информацию данными из внутренних и внешних источников. В решении представлены следующие источники обогащения:

   - константы;
   - cybertrace;
   - словари;
   - dns;
   - события;
   - ldap;
   - шаблоны;
   - данные о часовых поясах;
   - геоданные.

   Правила преобразования позволяют преобразовать содержимое поля события в соответствии с заданными условиями. В решении представлены следующие методы преобразования:

   - lower – перевод всех символов в нижний регистр;
   - upper – перевод всех символов в верхний регистр;
   - regexp – извлечение подстроки с использованием регулярных выражений RE2;
   - substring – получение подстроки по заданным номерам начальной и конечной позиции;
   - replace – замена текста введенной строкой;
   - trim – удаление заданных символов;
   - append – добавление символов в конец значения поля;
   - prepend – добавление символов в начало значения поля.

5. **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.

6. **Передача нормализованных событий**

   По завершении всех этапов обработки событие отправляется в настроенные точки назначения.

Коррелятор

Коррелятор – это компонент решения, 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:

- выявление алертов;
- уведомление о выявленных алертах;
- 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, решение 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 корреляционного правила могут использоваться другими корреляционными правилами.

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 решение будет выполнять при выявлении алерта. В решении 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, решение создает корреляционное событие и отправляет его в хранилище. На этом обработка события коррелятором завершается.

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.

Основные сущности

В этом разделе описаны основные сущности, с которыми работает KUMA.

Тенант

В KUMA действует режим мультитенантности, при котором один экземпляр решения KUMA, установленный в инфраструктуре основной организации (далее "главный тенант"), позволяет ее изолированным филиалам (далее "тенантам") получать и обрабатывать свои события.

Управление системой происходит централизовано через общий веб-интерфейс, при этом тенанты работают независимо друг от друга и имеют доступ только к своим ресурсам, сервисам и параметрам. События тенантов хранятся раздельно.

Пользователи могут иметь доступ сразу к нескольким тенантам. При этом можно выбирать, данные каких тенантов будут отображаться в разделах веб-интерфейса KUMA.

По умолчанию в KUMA созданы два тенанта:

- Главный (или Main) – в нем содержатся ресурсы и сервисы, относящиеся к главному тенанту. Эти ресурсы доступны только главному администратору.

- Общий (или Shared) – в этот тенант главный администратор может поместить ресурсы, категории активов и политики мониторинга, которые смогут задействовать пользователи всех тенантов. Доступ к Общему тенанту можно **ограничить** для отдельных пользователей.

  Если в параметрах пользователя установлен флажок **Скрывать ресурсы из общего тенанта**, этому пользователю становится недоступна принадлежащая Общему тенанту папка Shared в веб-интерфейсе KUMA в разделе **Ресурсы** → **<Тип ресурсов>**. Это означает, что пользователь не сможет просмотреть, отредактировать или еще как-то использовать общие ресурсы. Пользователь также не сможет экспортировать общие ресурсы и наборы ресурсов, в состав которых входят ресурсы из Общего тенанта: ни через веб-интерфейс, ни через REST API.

  При этом, если какие-то из доступных пользователю сервисов используют общие ресурсы, пользователь будет видеть название этих ресурсов в параметрах сервиса, но не сможет их просмотреть или изменить. Содержимое активных листов пользователю будет доступно, даже если ресурс этого активного листа является общим.

  Ограничение не распространяется на общие категории активов. Также общие ресурсы всегда доступны пользователям с ролью главного администратора.

Событие

События – это события информационной безопасности, зарегистрированные на контролируемых элементах IT-инфраструктуры организации. Например, события включают попытки входа в систему, взаимодействия с базой данных и рассылку информации с датчиков. Каждое отдельное событие может показаться бессмысленным, но если рассматривать их вместе, они формируют более широкую картину сетевой активности, помогающую 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 возможную угрозу безопасности, KUMA создает алерт: это оповещение об угрозе, к которому привязываются все относящиеся к нему данные и которое требует внимания специалиста по безопасности. Если характер поступающих в KUMA данных, создаваемых корреляционных событий и алертов указывает на возможную атаку или уязвимость, признаки такого происшествия можно объединить в инцидент.

Для обеспечения удобства расследования алертов и обработки инцидентов убедитесь, что на всех устройствах, связанных с жизненным циклом обработки событий (источники событий, серверы KUMA, клиентские хосты) время синхронизируется при помощи серверов Network Time Protocol (NTP).

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

   По завершении 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. Корреляционное событие. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, решение 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, и 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.

Алерт

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 обнаружений можно создать инциденты.

Работа с алертами в KUMA описана в этом разделе.

Инцидент

Если характер поступающих в KUMA данных, создаваемых корреляционных событий и алертов указывает на возможную атаку или уязвимость, признаки такого происшествия можно объединить в *инцидент*. Это позволяет специалистам 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.

Активы

Активы – это сетевые устройства, зарегистрированные в KUMA. Активы генерируют сетевой трафик при отправке и получении данных. Решение KUMA может быть настроено для отслеживания этой активности и создания базовых событий с четким указанием того, откуда исходит трафик и куда он направляется. В событии могут быть записаны исходные и целевые IP-адреса, а также DNS-имена. Если вы регистрируете актив с определенными параметрами (например, конкретным IP-адресом), формируется связь между этим активом и всеми событиями, в которых указаны эти параметры (в нашем случае IP-адрес).

Активы можно разделить на логические группы. Это позволяет создать прозрачную структуру вашей сети, а также дает дополнительные возможности при работе с правилами корреляции. Когда обрабатывается событие, к которому привязан актив, категория этого актива также принимается во внимание. Например, если вы присвоите высокий уровень важности определенной категории активов, то связанные с этими активами базовые события породят корреляционные события с более высоким уровнем важности. Это, в свою очередь, приведет к появлению обнаружений с более высоким уровнем важности и, следовательно, более быстрой реакцией на такой алерт.

Рекомендуется регистрировать сетевые активы в KUMA, поскольку их использование позволяет формулировать четкие и универсальные правила корреляции для более эффективного анализа событий.

Работа с активами в KUMA описана в этом разделе.

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 KUMA

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 веб-интерфейса 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 агента или хранилища могут быть установлены сразу на нескольких устройствах.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Агенты KUMA

Агенты KUMA – это сервисы, которые используются для пересылки необработанных событий с серверов и рабочих станций в точки назначения KUMA.

Типы агентов:

- wmi – используются для получения данных с удаленных устройств Windows с помощью Windows Management Instrumentation. Устанавливается на устройства Windows.
- wec – используются для получения журналов Windows с локального устройства с помощью Windows Event Collector. Устанавливается на устройства Windows.
- tcp – используются для получения данных по протоколу TCP. Устанавливается на устройства Linux и Windows.

- udp – используются для получения данных по протоколу UDP. Устанавливается на устройства Linux и Windows.
- nats-jetstream – используются для коммуникации через NATS. Устанавливается на устройства Linux и Windows.
- kafka – используются для коммуникации с помощью kafka. Устанавливается на устройства Linux и Windows.
- http – используются для связи по протоколу HTTP. Устанавливается на устройства Linux и Windows.
- file – используются для получения данных из файла. Устанавливается на устройства Linux и Windows.
- ftp – используются для получения данных по протоколу File Transfer Protocol. Устанавливается на устройства Linux и Windows.
- nfs – используются для получения данных по протоколу Network File System. Устанавливается на устройства Linux и Windows.
- snmp – используются для получения данных с помощью Simple Network Management Protocol. Устанавливается на устройства Linux и Windows.
- diode – используются вместе с диодами данных для получения событий из изолированных сегментов сети. Устанавливается на устройства Linux и Windows.
- etw – используются для получения данных Event Tracing for Windows. Устанавливается на устройства Windows.

Уровни важности

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

Если событие связано с активами, система использует наивысшую важность категории активов для расчета уровня важности корреляционного события или алерта.

Пример формулы для расчета уровня важности:

- Если к корреляционному событию или алерту не привязаны активы с уровнем важности или не привязаны активы вообще, в этом случае:
  - **Уровень важности корреляционного события** = **Уровень важности правила корреляции**.
  - **Уровень важности алерта** = **Уровень важности правила корреляции**.
- Если к событию или алерту привязано несколько активов, то **наивысшей важностью категории активов** считается самый высокий уровень важности категории активов, связанных с этим событием или активом. Если это значение больше уровня важности правила корреляции, в этом случае:
  - **Уровень важности корреляционного события** = (**Уровень важности правила корреляции** + **Наивысшая важность категории активов** + 1) / 2.
  - **Уровень важности алерта** = (**Уровень важности правила корреляции** + **Наивысшая важность категории активов** + 1) / 2.

Уровень важности корреляционного события не может быть ниже уровня важности правила корреляции. Коррелятор и коллектор должны находиться в том же тенанте, что и активы. Уровни важности активов других тенантов не учитываются.

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

Возможные значения уровня важности:

- 1 – Низкий
- 2 – Средний
- 3 – Высокий
- 4 – Критический

Лицензирование решения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием решения.

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Перейти в директорию с распакованным установщиком и прочитать текстовый файл `./roles/kuma/files/LICENSE`.
- Перейти в директорию с распакованным установщиком и выполнить следующую команду, чтобы вывести на экран текст Лицензионного соглашения:

  ```
  ./roles/kuma/files/kuma license --show
  ```

- На хосте с любым установленным компонентом KUMA, таким как Ядро KUMA, коллектор, коррелятор, хранилище, выполнить следующую команду, чтобы вывести на экран текст Лицензионного соглашения:

  ```
  /opt/kaspersky/kuma/kuma license --show
  ```

- На устройствах, входящих в группы kuma_storage, kuma_collector, kuma_correlator или kuma_core в файле инвентаря, открыть файл LICENSE, расположенный в директории `/opt/kaspersky/kuma`.

  На хосте из группы kuma_core можно увидеть Лицензионное соглашение, только если выбрана не кластерная установка.

- На Windows-агенте выполнить следующую команду, чтобы вывести на экран текст Лицензионного соглашения:

  ```
  .\kuma.exe license --show
  ```

- На Linux-агенте перейти в директорию с исполняемым файлом agent и выполнить следующую команду, чтобы вывести на экран текст Лицензионного соглашения:

  ```
  ./agent license --show
  ```

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

О лицензии

Лицензия – это ограниченное по времени право на использование решения, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование решения в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования решения зависят от типа лицензии, по которой было активировано решение.

Лицензия предоставляется при приобретении решения. Поведение KUMA в случае отсутствия лицензии:

- По истечении срока действия лицензии KUMA продолжает работу, но с ограниченной функциональностью: коллекторы продолжают принимать и обрабатывать события в течение 7 суток, а потом перезагружаются и перестают принимать новые события. Старые события остаются доступны. Также невозможно создавать и редактировать ресурсы, создавать и запускать сервисы.
- Если лицензионный ключ удален, коллекторы KUMA прекращают принимать и обрабатывать новые события сразу. Старые события доступны. Также невозможно создавать и редактировать ресурсы, создавать и запускать сервисы.

Чтобы продолжить использование KUMA в режиме полной функциональности, вам нужно продлить срок действия лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о решении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, количество обрабатываемых событий в секунду);
- дата начала срока действия лицензии;

- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

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

Для активации решения вы можете добавить лицензионный ключ, применив *код активации* или *файл ключа*, которые предоставлены вам после приобретения лицензии. Лицензионный ключ отображается в интерфейсе решения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в решение.

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

Лицензионный ключ может быть активным и резервным.

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

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование решения, 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 файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения KUMA.

Чтобы активировать решение 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.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр, которая позволяет активировать решение. Вы получаете код активации от "Лаборатория Касперского" по указанному вами адресу электронной почты после приобретения KUMA.

Чтобы активировать решение с помощью кода активации, серверу с установленным Ядром KUMA требуется доступ в интернет для подключения к серверу активации "Лаборатории Касперского" по адресу https://activation-v2.kaspersky.com:443.

В случае закрытой инфраструктуры вы можете указать прокси-сервер.

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

При удалении кода активации из KUMA коллекторы KUMA прекращают принимать и обрабатывать новые события сразу. Старые события доступны. Также невозможно создавать и редактировать ресурсы, создавать и запускать сервисы.

Если вы активировали решение с помощью файла ключа и добавляете новый код активации, активация с помощью кода активации будет выполнена бесшовно, если параметры кода активации полностью соответствуют параметрам файла ключа. Если в параметрах есть различия, будет выполнена перезагрузка сервисов.

KUMA генерирует аудит события по факту добавления лицензионного ключа, удаления лицензионного ключа, истечения срока лицензии.

При переходе с файла ключа на код активации прежний лицензионный ключ будет удален автоматически. Прежде чем обновлять лицензию, убедитесь, что прежний файл ключа есть у вас в доступе.

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 "решение") – 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.
    - По расписанию: из Kaspersky Security Center и KICS/KATA.
  - Создать активы вручную через веб-интерфейс или с помощью API.

  KUMA хранит следующие данные об устройствах:

  - Технические характеристики устройства.
  - Уязвимости, зафиксированные на активе.
  - Данные, специфичные для источника получения актива.

- Дополнительные технические характеристики устройств в сети организации, указываемые пользователем для отправки инцидента в НКЦКИ: IP-адреса, доменные имена, URI-адреса, адрес электронной почты атакованного объекта, атакованная сетевая служба и порт/протокол.

- Данные, получаемые от ГосСОПКА и из сообщений от НКЦКИ: данные об организации субъекта ГосСОПКА, категория и тип события, технические сведения о вредоносной системе (включая доменное имя, IP-адреса, хеш-сумму, URI-адрес, адрес электронной почты), информация об уязвимости программы, подвергшейся атаке, и информация об атакованном объекте.

- Данные организации: наименование, ИНН, адрес, адрес электронной почты для отправки информации об уведомлении.

- 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, базу поиска (Base DN), учетные данные для подключения и сертификат в консоли KUMA.

- 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. Дополнительно можно настроить сохранение адреса или имя хоста сервера-агрегатора событий.

- Данные, необходимые для интеграции KUMA с другими приложениями (Kaspersky Threat Lookup, Kaspersky CyberTrace, Kaspersky Security Center, Kaspersky Industrial CyberSecurity for Networks, Kaspersky Automated Security Awareness Platform, Kaspersky Endpoint Detection and Response, Security Orchestration, Automation and Response SOAR, AI-сервисы: AI рейтинг и статус активов, Kaspersky Investigation & 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, адрес электронной почты. Пользователь вводит эти данные в консоли KUMA

- Данные об источниках, с которых настроено получение событий.

  Это могут быть название источника, имя хоста, 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(-и).

  - 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-адрес контроллера домена, сертификат (публичный ключ root, которым подписан сертификат AD), полный путь к группе доступа пользователей в AD (distinguished name).

  - Active Directory Federation Services: 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: база поиска (Base DN), URL, сертификат (публичный ключ root, которым подписан сертификат FreeIPA), учетные данные пользовательской интеграции, учетные данные для подключения.

- События 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".

- Данные по действующим лицензиям в KUMA.

- 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.

Перечисленные данные хранятся в базе данных KUMA (ClickHouse, 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.

Добавление лицензионного ключа

Вы можете добавить лицензионный ключ в веб-интерфейсе KUMA. Если вы активируете решение с помощью файла ключа, то лицензионных ключей может быть два – активный и резервный. Если же вы используете код активации, лицензионный ключ будет один. В KUMA группа из активного и резервного лицензионных ключей или одного кода активации называется *группой лицензий*. Соответственно, вы можете добавить группу лицензий либо с помощью двух файлов ключей, либо с помощью кода активации.

Если в один экземпляр KUMA добавлено несколько групп лицензий, активные лицензионные ключи всех групп лицензий автоматически объединяются. В результате создается *объединенная лицензия*. Лицензионные ключи такой лицензии объединяются по следующим правилам:

- Значения параметра **Доступное EPS** всех активных лицензионных ключей суммируются. Итоговое значение EPS прописывается в объединенной лицензии и становится доступным всем тенантам.

  При истечении срока действия какого-либо лицензионного ключа, входящего в объединенную лицензию, значение ограничения EPS этого лицензионного ключа будет автоматически вычтено из суммарного значения EPS объединенной лицензии. Соответственно, при добавлении нового активного лицензионного ключа в объединенную лицензию значение ограничения EPS этого лицензионного ключа будет автоматически прибавлено к суммарному значению EPS.

- Набор модулей, доступных в лицензиях тенантов, должен совпадать. Если в какой-то лицензии присутствует модуль, недоступный в других лицензиях, этот модуль не будет доступен в объединенной лицензии. Соответственно, такой модуль не будет доступен ни для одного тенанта.

  Это же правило справедливо при добавлении в объединенную лицензию новых лицензионных ключей. Если в новом лицензионном ключе будет доступен модуль, недоступный в объединенной лицензии, этот модуль не будет доступен в рамках объединенной лицензии. Если в новом лицензионном ключе будет недоступен какой-то модуль, доступный в объединенной лицензии, этот модуль станет недоступным в рамках объединенной лицензии. При добавлении лицензионного ключа с несовпадающим набором модулей, KUMA отображает предупреждение и добавит такой лицензионный ключ только после вашего подтверждения.

- Объединенная лицензия может включать до 50 активных ключей.

Только пользователи с уровнем прав *Управление* на функциональную область *Лицензия* могут добавлять лицензионный ключ. Из предустановленных ролей такое право имеет только Главный администратор.

Как добавить лицензионный ключ

1. В веб-интерфейсе KUMA выберите раздел **Параметры** → **Другое** → **Лицензия**.

   Откроется окно со списком добавленных групп лицензий.

2. Нажмите на кнопку **Добавить группу лицензий**.

3. В открывшемся окне введите название группы лицензий.

4. Нажмите на кнопку **Добавить**.

   Новая группа лицензий отобразится в списке.

5. Нажмите на название добавленной группы лицензий.

   Откроется окно настройки группы лицензий.

6. Выберите способ добавления лицензионного ключа:

   - С помощью кода активации:

     a. Укажите код активации.

     b. Если в компании при подключении к интернету используется прокси-сервер, укажите его параметры. Для активации решения потребуется подключение к интернету.

- С помощью файла ключа:

  a. В разделе **Активный лицензионный ключ** нажмите на кнопку **Загрузить**, затем выберите файл ключа (файл с расширением KEY).

  b. В разделе **Резервный лицензионный ключ** аналогичным образом добавьте резервный лицензионный ключ.

7. Нажмите на кнопку **Добавить**.

Лицензионный ключ добавлен.

Как заменить активный лицензионный ключ

1. Удалите текущий лицензионный ключ.

2. Добавьте новый лицензионный ключ (см. инструкцию выше).

Как в группу лицензий добавить резервный лицензионный ключ

1. В веб-интерфейсе KUMA выберите раздел **Параметры** → **Другое** → **Лицензия**.

   Откроется окно со списком добавленных групп лицензий.

2. Нажмите на название группы лицензий, в которую вы хотите добавить резервный лицензионный ключ.

3. В открывшемся окне в разделе **Резервный лицензионный ключ** нажмите на кнопку **Загрузить**, затем выберите файл ключа (файл с расширением KEY).

4. Нажмите на кнопку **Добавить**.

Пример использования объединенной лицензии

В этом примере рассматривается использование объединенной лицензии в холдинге, состоящем из компаний A, B и C. В холдинге развернут и активирован один экземпляр KUMA, настроена мультитенантность. Невозможно настроить мультитенантнсть, не активировав решение, так как без активации невозможно создавать сервисы и ресурсы.

Необходимо, чтобы каждая из компаний A, B и C впоследствии приобретала свою лицензию на использование решения.

Для решения этой задачи используйте объединенную лицензию:

1. Каждая из компаний A, B и C приобретает лицензию на использование решения в виде лицензионного сертификата и файла ключа или кода активации.

2. Получите от компаний A, B и C файлы ключа и/или коды активации для активации решения.

3. С помощью предоставленных компаниями A, B и C файлов ключа и/или кодов активации добавьте три активных лицензионных ключа (см. инструкцию выше).

Лицензионные ключи, добавленные в процессе развертывания решения и в шаге 3 сценария, автоматически объединятся. В результате будет создана объединенная лицензия, данные о которой отобразятся в разделе **Параметры** → **Другое** → **Лицензия** над списком групп лицензий.

Просмотр информации о добавленном лицензионном ключе

.Вы можете просмотреть информацию о добавленном лицензионном ключе в веб-интерфейсе KUMA в разделе **Параметры** → **Другое** → **Лицензия**.

> Только пользователи с уровнем прав *Чтение* или *Управление* на функциональную область *Лицензия* могут просматривать информацию о лицензии. Из предустановленных ролей такое право имеет только Главный администратор.

В окне вкладки **Лицензия** отображается следующая информация о добавленных лицензионных ключах:

- **Наименование лицензионного ключа**. Содержит название решения и уточняющие параметры, если применимо.
- Уникальная буквенно-цифровая последовательность лицензионного ключа.
- **Доступное EPS** – количество обрабатываемых в секунду событий, которое поддерживается лицензией.
- **Текущее** – текущее среднее количество уникальных обрабатываемых событий за 24 часа, подсчитанное с помощью метода скользящего окна. Каждые 15 секунд KUMA считает количество событий после их обработки коллектором (после фильтрации и агрегации на выходе из коллектора) до среднего EPS в час, а затем – в сутки.
- **Текущий EPS за час** – текущее среднее количество событий в час, которое обрабатывает KUMA.

  > Параметры **Текущее** и **Текущий EPS за час** доступны только для лицензий SMART I и SMART II. Если значения этих двух параметров превышены, коллектор с максимальным количеством EPS останавливает прием новых событий на один час. По прошествии одного часа работа коллектора будет восстановлена. Может быть приостановлена работа нескольких коллекторов. Пользователю с ролью Главный администратор будет отправлено уведомление о превышении допустимого лицензией количества EPS. Ограничения действуют только для лицензий SMART I и SMART II.

- **Дата истечения срока действия** – дата истечения срока действия лицензионного ключа.
- **Срок** – количество дней до истечения срока действия лицензии.
- **Модули** – модули, доступные по лицензии.

Удаление лицензионного ключа

Вы можете удалить добавленный лицензионный ключ из KUMA (например, если вам нужно заменить текущий лицензионный ключ другим). После удаления лицензионного ключа коллекторы сразу прекращают принимать и обрабатывать события. Старые события остаются доступны. Также невозможно создавать и изменять ресурсы, создавать и запускать сервисы. Эта работа возобновится после добавления лицензионного ключа.

Только пользователи с уровнем прав *Управление* на функциональную область *Лицензия* могут удалять лицензионный ключ. Из предустановленных ролей такое право имеет только Главный администратор.

Чтобы удалить лицензионный ключ, удалите группу лицензий, в которую добавлен лицензионный ключ:

1. В веб-интерфейсе KUMA выберите раздел **Параметры** → **Другое** → **Лицензия**.

   Откроется окно со списком добавленных групп лицензий.

2. С помощью флажка слева от названия выберите группу лицензий, в которую входит лицензионный ключ, который вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

4. Подтвердите удаление группы лицензий.

Лицензионный ключ удален из решения.

Руководство администратора

В этой главе представлена информация об установке и настройке SIEM-системы KUMA.

Установка и удаление KUMA

Для выполнения установки вам понадобится дистрибутив:

- **kuma-ansible-installer-<номер сборки>.tar.gz** содержит все необходимые файлы для установки KUMA без использования Kubernetes. Доступна распределенная установка с Ядром KUMA в кластере на основе алгоритма Raft (далее — "в кластере Raft").

- **kuma-ansible-installer-k8s-<номер сборки>.tar.gz** содержит все необходимые файлы для установки KUMA в отказоустойчивой конфигурации на базе Kubernetes.

Для установки вам понадобится файл установщика install.sh и файл инвентаря с описанием инфраструктуры. Файл инвентаря вы сможете создать на основе шаблона. Каждый дистрибутив содержит файл установщика install.sh и следующие шаблоны файла инвентаря:

- single.inventory.yml.template

- distributed.inventory.yml.template

- expand.inventory.yml.template

- k0s.inventory.yml.template

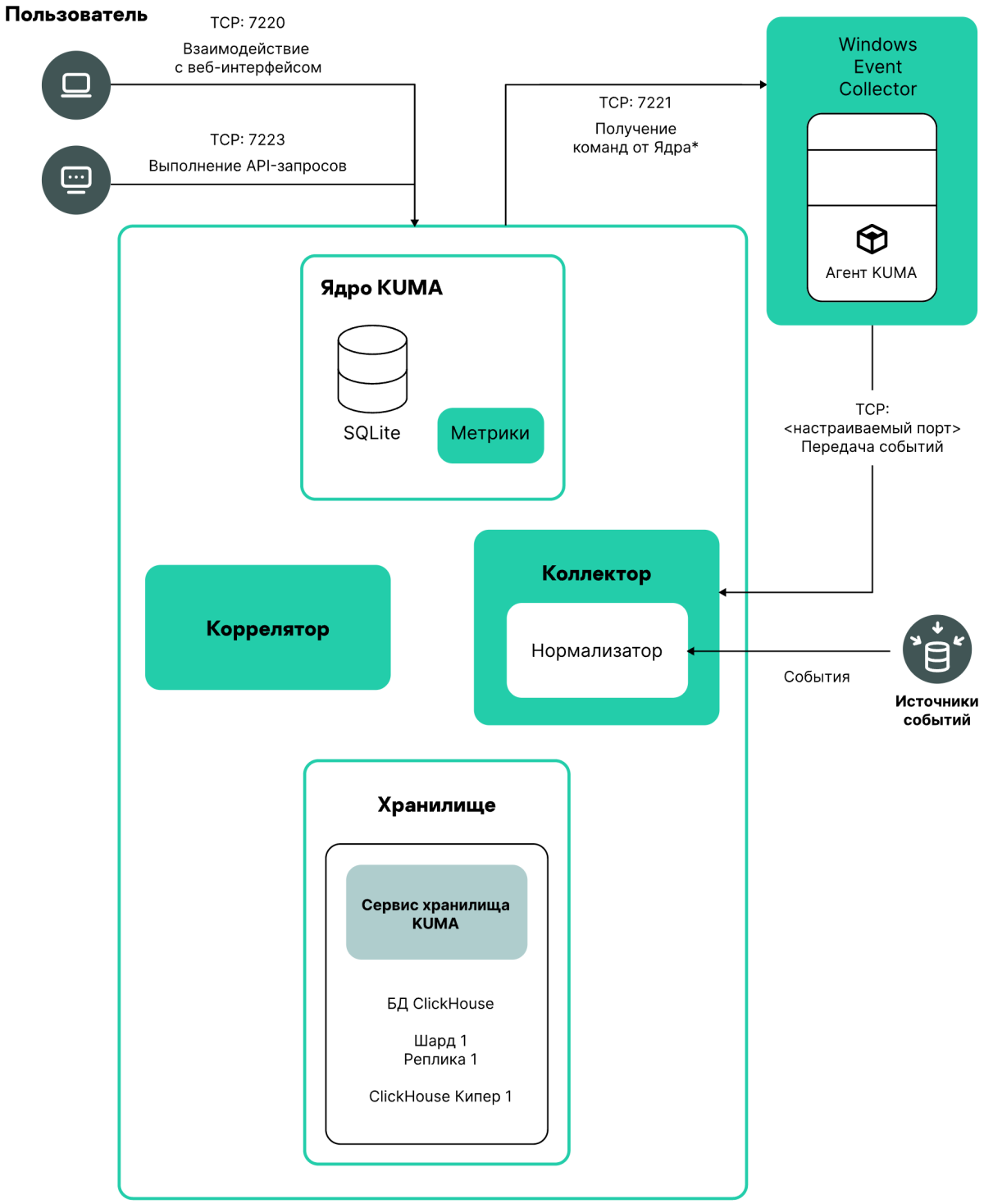
KUMA размещает свои файлы в папке /opt, поэтому мы рекомендуем сделать /opt отдельным разделом и выделить под него все дисковое пространство, за исключением 16 ГБ для операционной системы.

Установка KUMA выполняется одинаково на всех хостах при помощи установщика и подготовленного вами файла инвентаря, в котором описана конфигурация. Мы рекомендуем заранее продумать схему установки.

Доступны следующие варианты установки:

- Установка на одном сервере

Схема установки на одном сервере



*-7221 и другие порты для установки сервисов, которые вы указываете в качестве значения параметра --api.point <порт>

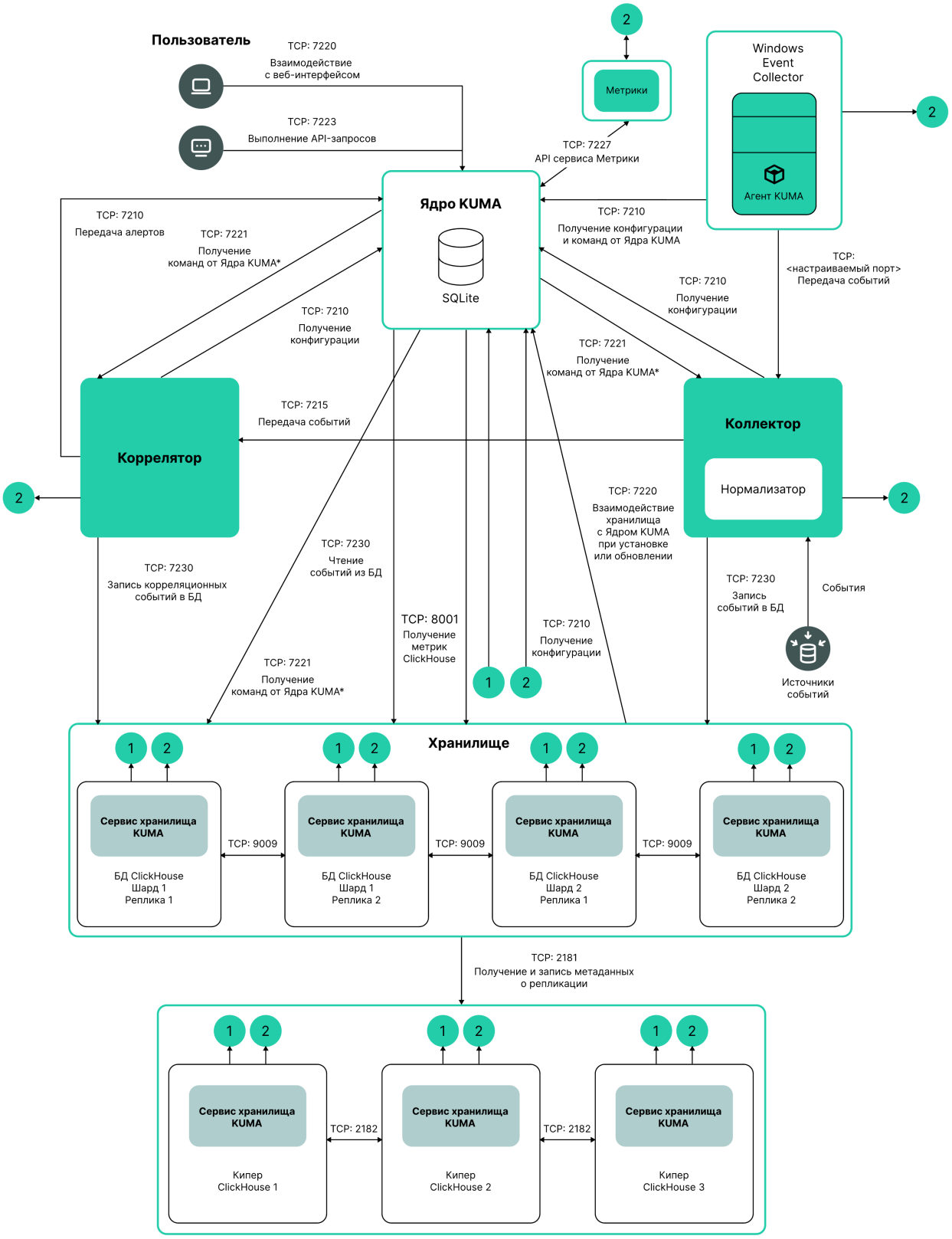
Пример файла инвентаря для схемы установки на одном сервере

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: true
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
    ansible_user: <пользователь из группы sudo>
    ansible_become: true
    ansible_port: 2222
  children:
    kuma_core:
      hosts:
        kuma1.example.com:
    kuma_collector:
      hosts:
        kuma1.example.com
    kuma_correlator:
      hosts:
        kuma1.example.com
    kuma_storage:
      hosts:
        kuma1.example.com:
          shard: 1
          replica: 1
          keeper: 1
    kuma_metrics:
      hosts:
        kuma1.example.com
```

Вы можете установить все компоненты KUMA на одном сервере: в файле инвентаря single.inventory.yml для всех компонентов следует указывать один сервер. Установка "все в одном" может обеспечить обработку небольшого потока событий - до 10000 EPS. Если вы планируете использовать много макетов панели мониторинга и обрабатывать большой объем поисковых запросов, одного сервера может не хватить. Мы рекомендуем выбрать распределенную установку.

- Распределенная установка

Схема распределенной установки



*~7221 и другие порты для установки сервисов, которые вы указываете в качестве значения параметра --api.point <порт>

Схема распределенной установки

Пример файла инвентаря для схемы распределенной установки

```
all:
```

```
    vars:
      deploy_to_k8s: false
      need_transfer: false
      generate_etc_hosts: false
      deploy_example_services: false
      no_firewall_actions: false
  kuma:
    vars:
      ansible_connection: ssh
      ansible_user: root
    children:
      kuma_core:
        hosts:
          kuma-core-1.example.com:
            ip: 0.0.0.0
      kuma_collector:
        hosts:
          kuma-collector-1.example.com:
            ip: 0.0.0.0
      kuma_correlator:
        hosts:
          kuma-correlator-1.example.com:
            ip: 0.0.0.0
      kuma_storage:
        hosts:
          kuma-storage-cluster1-server1.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server2.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server3.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server4.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server5.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 1
          kuma-storage-cluster1-server6.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 2
          kuma-storage-cluster1-server7.example.com:
            ip: 0.0.0.0
            shard: 0
```

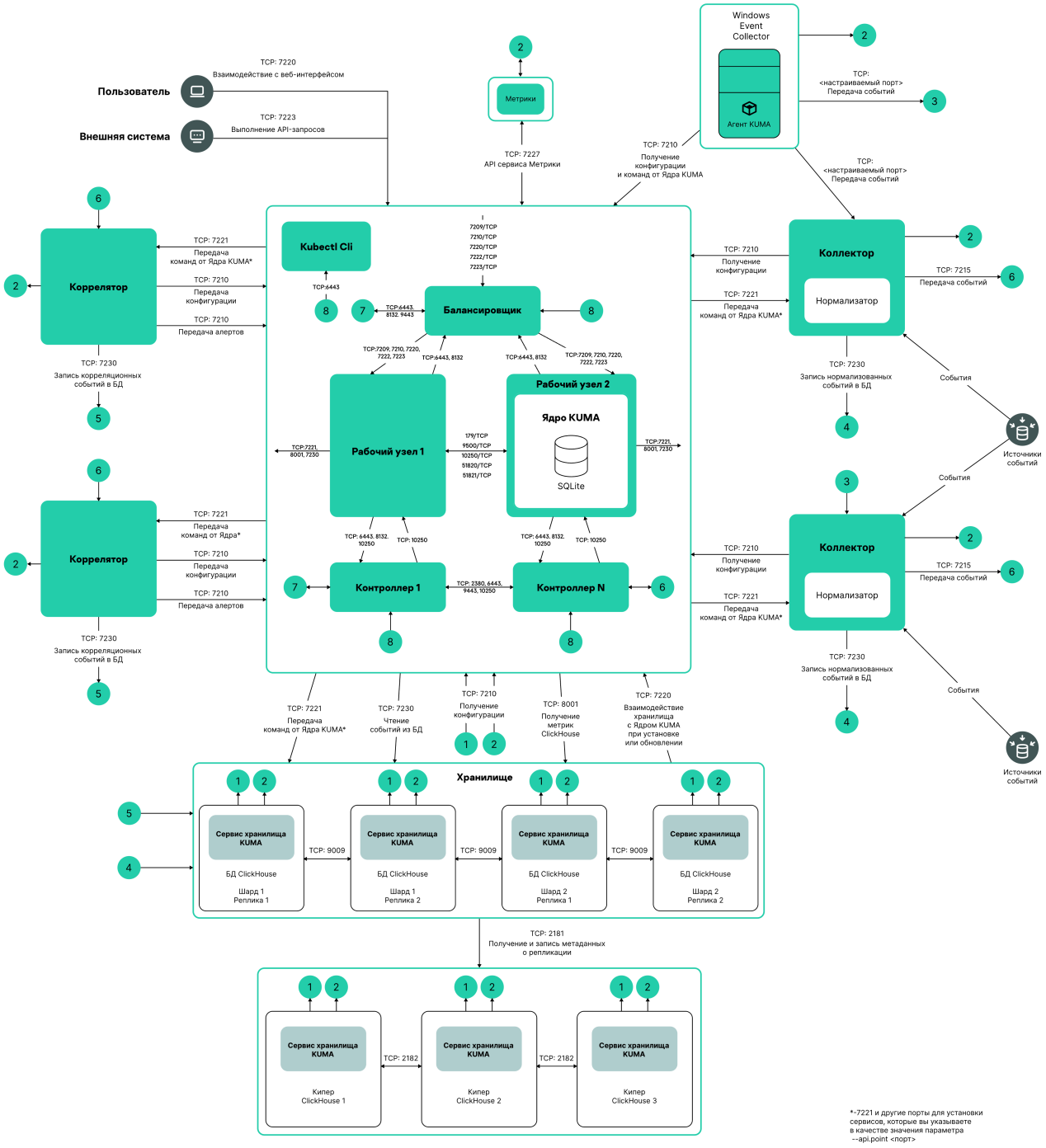
```
        replica: 0
        keeper: 3
```

Вы можете установить сервисы KUMA на разных серверах: конфигурацию для распределенной установки вы можете описать в файле инвентаря distributed.inventory.yml.

- Установка в отказоустойчивой конфигурации:

  - Распределенная установка с Ядром KUMA в кластере Kubernetes

    Схема распределенной установки с Ядром KUMA в кластере Kubernetes



Распределенная установка в отказоустойчивой конфигурации

Пример файла инвентаря для схемы распределенной установки с Ядром KUMA в кластере Kubernetes

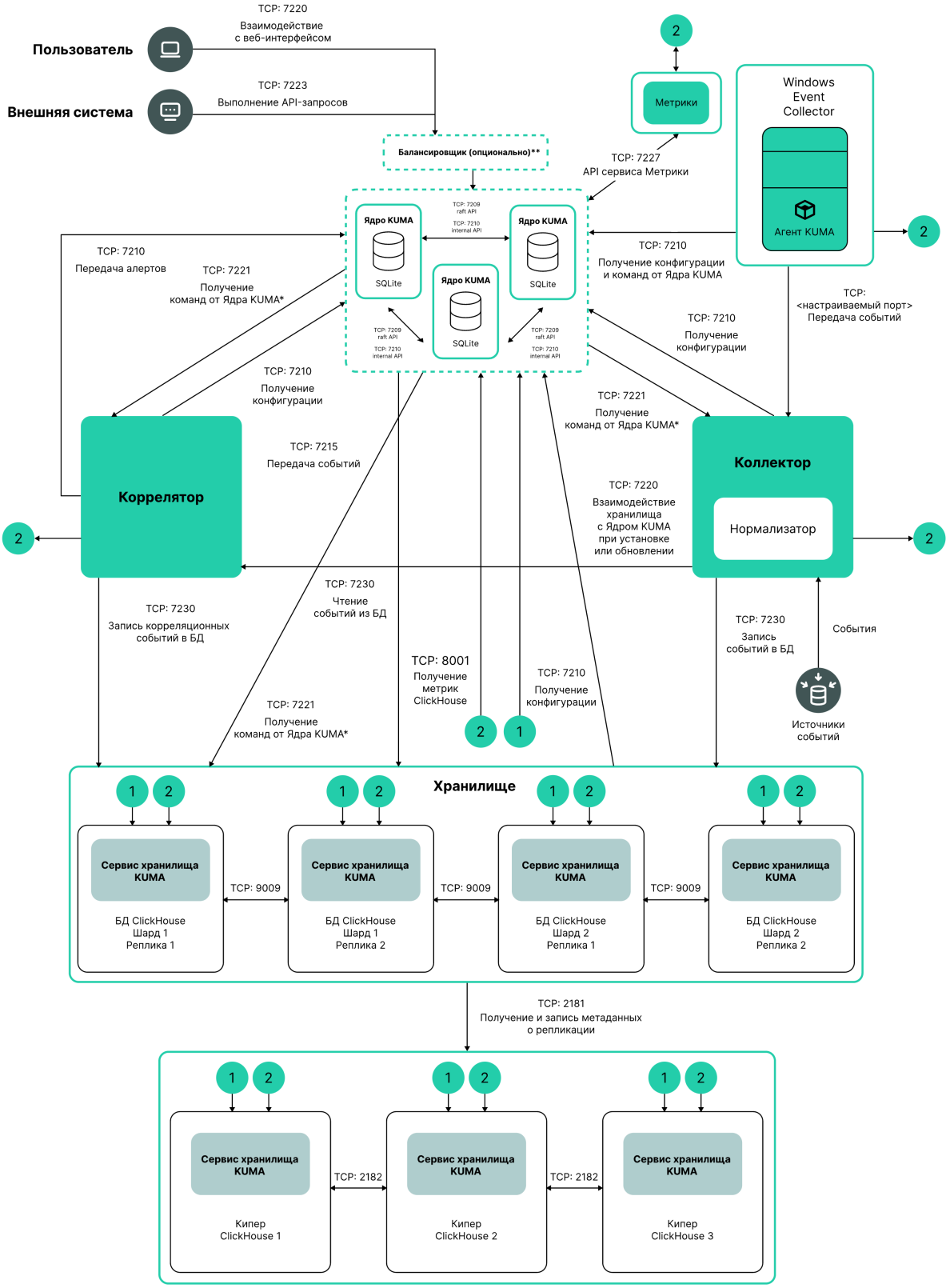
```
all:
  vars:
    deploy_to_k8s: true
    need_transfer: true
    generate_etc_hosts: false
    airgap: true
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
        kuma-collector-2.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
        kuma-correlator-2.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
```

```
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
kuma_k0s:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_lb:
      hosts:
        kuma_lb.example.com:
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp1.example.com:
          ansible_host: 10.0.1.11
        kuma_cp2.example.com:
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
        kuma-core-1.example.com:
          ansible_host: 10.0.1.13
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
        kuma_worker2.example.com:
          ansible_host: 10.0.1.14
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

Вы можете установить Ядро KUMA в кластере Kubernetes для обеспечения отказоустойчивости. Используйте файл инвентаря k0s.inventory.yml для описания конфигурации.

- Распределенная установка с Ядром KUMA в кластере Raft

Схема распределенной установки с Ядром KUMA в кластере Raft



*-7221 и другие порты для установки сервисов, которые вы указываете в качестве значения параметра --api.point <порт>

**Все сервисы KUMA могут обращаться напрямую к сервисам Ядра KUMA, как показано на схеме, и могут взаимодействовать с кластером через балансировщик.

Пример файла инвентаря distributed.inventory.yml для первоначальной установки

```
all:
```

```
    vars:
      deploy_to_k8s: false
      need_transfer: false
      generate_etc_hosts: false
      deploy_example_services: false
      no_firewall_actions: false
  kuma:
    vars:
      ansible_connection: ssh
      ansible_user: root
    children:
      kuma_core:
        hosts:
          kuma-core-1.example.com:
            ip: 0.0.0.0
            raft_node_addr: ""
      kuma_core_peers:
        hosts:
          kuma-core-2.example.com:
            ip: 0.0.0.0
          kuma-core-3.example.com:
            ip: 0.0.0.0
      kuma_collector:
        hosts:
          kuma-collector-1.example.com:
            ip: 0.0.0.0
      kuma_correlator:
        hosts:
          kuma-correlator-1.example.com:
            ip: 0.0.0.0
      kuma_storage:
        hosts:
          kuma-storage-cluster1-server1.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server2.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server3.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server4.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server5.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 1
          kuma-storage-cluster1-server6.example.com:
```

```
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

Пример файла инвентаря для расширения кластера с помощью установщика expand.sh

```
kuma:
  vars:
    no_firewall_actions: false
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core_peers:
      hosts:
        kuma-core-4.example.com:
          ip: 0.0.0.0
        kuma-core-5.example.com:
          ip: 0.0.0.0
```

Вы можете установить несколько Ядер KUMA в кластере Raft для репликации данных и обеспечения отказоустойчивости в распределенной системе. Используйте файл инвентаря distributed.inventory.yml для описания конфигурации.

Требования к установке решения

Общие требования к установке решения

Вы можете установить решение на следующих операционных системах:

- Oracle Linux.
- Astra Linux.
- Ubuntu.
- РЕД ОС.
- МосОС.

  Поддерживаемые версии операционных систем указаны в разделе Аппаратные и программные требования.

  Поддерживаются конфигурации Сервер и Сервер с поддержкой графического интерфейса. В конфигурации Сервер с поддержкой графического интерфейса не требуется устанавливать дополнительные пакеты для формирования отчетов.

Операционная система РЕД ОС 8 поддерживается без высокой доступности (англ. High Availability, HA). При использовании операционной системы РЕД ОС 8 в конфигурации Сервер с поддержкой графического интерфейса вам нужно установить пакет iscsi-initiator-utils, после чего выполнить следующие команды:

```
systemctl enable iscsid
systemctl start iscsid
```

Перед развертыванием решения убедитесь, что выполнены следующие условия:

- Серверы, предназначенные для установки компонентов, соответствуют аппаратным и программным требованиям.
- Порты, которые KUMA займет при установке, доступны.
- Адресация компонентов KUMA осуществляется по полному доменному имени FQDN хоста в формате hostname.example.com. Перед установкой решения убедитесь, что выполнение следующей команды возвращает корректное имя FQDN хоста:

  ```
  hostname -f
  ```

- Имя сервера, на котором запускается установщик, отличается от `localhost` или `localhost.<домен>`.
- Имя сервера, на котором будет установлено Ядро KUMA, не начинается с цифры.
- Настроена синхронизация времени на всех серверах с сервисами KUMA по протоколу Network Time Protocol (NTP).
- На всех хостах, на которые будут установлены сервисы KUMA, нет пользователя с именем kuma. Такой пользователь создается автоматически при установке сервисов KUMA.

Требования к установке на устройствах с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, МосОС

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	МосОС
Версия Python	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.
Модуль SELinux	Выключен.	Выключен.	Выключен.	Выключен.	Выключен.

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	МосОС
Система управления пакетами	pip3.	pip3.	pip3.	pip3.	pip3.

Основные пакеты	• netaddr.
	• firewalld.
	Подробнее об обновлении с операционной системы Oracle Linux 8.x до Oracle Linux 9.x.
	Вы можете установить пакеты с помощью следующих команд:
	`pip3 install netaddr`
	`yum install firewalld`
		• python3-apt.
		• curl.
		• libcurl4.
		• ufw.
		Вы можете установить пакеты с помощью команды:
		`apt install python3-apt curl libcurl4 ufw`
			• python3-apt.
			• curl.
			• libcurl4.
			• ufw.
			Вы можете установить пакеты с помощью команды:
			`apt install python3-apt curl libcurl4 ufw`
				• netaddr.
				• firewalld.
				Вы можете установить пакеты с помощью следующих команд:
				`pip3 install netaddr`
				`dnf install firewalld`
					• python3-rpm
					• firewalld.
					Вы можете установить пакет с помощью следующих команд:
					`zypper refresh`
					`zypper install python3-rpm firewalld`

Зависимые пакеты	Нет значения.	• netaddr. • python3-cffi-backend. Вы можете установить пакеты с помощью команды: `apt install python3-netaddr python3-cffi-backend` Если вы планируете обращаться к базам данных Oracle DB из KUMA, вам нужно установить пакет Astra Linux libaio1.	• netaddr. • python3-cffi-backend. Вы можете установить пакеты с помощью команды: `apt install python3-netaddr python3-cffi-backend`	Нет значения.	Нет значения.
Пакеты, которые нужно установить на устройстве с Ядром KUMA для корректного формирования отчетов и возможности их скачивания	• nss. • gtk2. • atk. • libnss3.so. • libatk-1.0.so.0. • libxkbcommon. • libdrm. • at-spi2-atk. • mesa-libgbm. • alsa-lib. • cups-libs. • libXcomposite. • libXdamage. • libXrandr. Вы можете установить пакеты с помощью команды: `yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`	• libgtk2.0.0. • libnss3. • libatk-adaptor. • libdrm-common. • libgbm1. • libxkbcommon0. • libasound2. Вы можете установить пакеты с помощью команды: `apt install libgtk2.0.0 libnss3 libatk-adaptor libdrm-common libgbm1 libxkbcommon0 libasound2`	• libatk1.0-0. • libgtk2.0-0. • libatk-bridge2.0-0. • libcups2. • libxcomposite-dev. • libxdamage1. • libxrandr2. • libgbm-dev. • libxkbcommon-x11-0. • libpangocairo-1.0-0. • libasound2 (для Ubuntu 22.04 LTS) или libasound2t64 (для Ubuntu 24.04 LTS). Вы можете установить пакеты с помощью команды (для Ubuntu 22.04 LTS): `apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2` Для Ubuntu 24.04 LTS выполните команду:	• nss. • gtk2. • atk. • libnss3.so. • libatk-1.0.so.0. • libxkbcommon. • libdrm. • at-spi2-atk. • mesa-libgbm. • alsa-lib. • cups-libs. • libXcomposite. • libXdamage. • libXrandr. Вы можете установить пакеты с помощью команды: `dnf install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`	Нет значения.

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	МосОС
			`apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2t64`		
Уровень прав пользователя, необходимый для установки решения	Нет значения.	Вам нужно присвоить необходимый уровень прав пользователю, под которым вы собираетесь устанавливать решение, с помощью команды: `sudo pdpl-user -i 63 < имя пользователя, под которым вы собираетесь устанавливать решение >`	Нет значения.	Нет значения.	Нет значения.

Обновление Oracle Linux 8.x до Oracle Linux 9.x с установленными сервисами KUMA

Чтобы выполнить обновление с Oracle Linux 8.x до Oracle Linux 9.x:

1. Отключите сервисы KUMA на хостах, где сервисы установлены, с помощью следующих команд:
   - `sudo systemctl disable kuma-collector-< идентификатор сервиса >.service`
   - `sudo systemctl disable kuma-correlator-< идентификатор сервиса >.service`
   - `sudo systemctl disable kuma-storage-< идентификатор сервиса >.service`
   - `sudo systemctl disable kuma-metrics-< идентификатор сервиса metrics >.service`
   - `sudo systemctl disable kuma-vmalert.service`
   - `sudo systemctl disable kuma-core-< идентификатор сервиса Ядра KUMA >.service`
2. Выполните обновление ОС на каждом хосте.
3. Включите сервисы на хостах, где сервисы установлены, с помощью следующих команд:
   - `sudo systemctl enable kuma-core-< идентификатор сервиса Ядра KUMA >.service`
   - `sudo systemctl enable kuma-storage-< идентификатор сервиса >.service`
   - `sudo systemctl enable kuma-collector-< идентификатор сервиса >.service`
   - `sudo systemctl enable kuma-correlator-< идентификатор сервиса >.service`

- `sudo systemctl enable kuma-metrics-<идентификатор сервиса metrics>.service`
- `sudo systemctl enable kuma-vmalert.service`

4. Перезагрузите хосты.

В результате обновление выполнено.

Порты, используемые KUMA при установке

Для правильной работы решения нужно убедиться, что компоненты KUMA могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов KUMA.

Перед установкой KUMA убедитесь, что следующие порты свободны на хосте из секции `kuma_metrics` в файле инвентаря, где вы планируете устанавливать сервис Метрики:

- 7227.
- 7228.
- 8001.

В таблице ниже показаны значения сетевых портов по умолчанию. Порты открываются установщиком автоматически при установке KUMA

Сетевые порты, используемые для взаимодействия компонентов KUMA

Протокол	Порт	Направление	Назначение подключения
HTTPS	7222	От клиента KUMA к серверу с компонентом Ядро KUMA.	Реверс-прокси к системе CyberTrace.
HTTPS	8123	Локальные обращения от сервиса хранилища к локальному узлу кластера клика.	Запись и получение нормализованных событий в кластере ClickHouse.
HTTPS	9009	Между репликами кластера ClickHouse.	Внутренняя коммуникация между репликами кластера ClickHouse для передачи данных кластера.
TCP	2181	От узлов кластера ClickHouse к сервису координации репликации ClickHouse keeper.	Получение и запись репликами серверов ClickHouse метаинформации о реплицировании.
TCP	2182	От сервисов координации репликации ClickHouse keeper друг к другу.	Внутренняя коммуникация между сервисами координации репликации, используемая для достижения кворума.
TCP	7210	От всех компонентов KUMA на сервер Ядра KUMA.	Получение конфигурации KUMA от сервера Ядра KUMA, а также запись метрик работы агента KUMA.
TCP	7220	• От клиента KUMA к серверу с компонентом Ядро KUMA. • От хостов хранилищ к серверу с компонентом Ядро KUMA во время установки или обновления.	• Доступ пользователей к веб-интерфейсу KUMA. • Взаимодействие хостов хранилищ с Ядром KUMA при установке или обновлении. После установки или обновления порт можно закрыть.

TCP	7221 и другие порты, используемые для установки сервисов в качестве значения параметра --api.port <порт>	От Ядра KUMA к сервисам KUMA.	Администрирование сервисов из веб-интерфейса KUMA.
TCP	7223	К серверу Ядра KUMA.	Порт, используемый по умолчанию для API-запросов.
TCP	8001	От сервиса Метрики к серверу ClickHouse.	Получение метрик работы сервера ClickHouse.
TCP	9000	• Исходящие и входящие соединения между серверами кластера ClickHouse. • От локального клиента client.sh к локальному узлу кластера.	Порт собственного протокола ClickHouse (также называется *протокол ClickHouse TCP*). Используется приложениями и процессами ClickHouse, такими как clickhouse-server, clickhouse-client, а также собственными инструментами ClickHouse. Используется для распределенных запросов при взаимодействии между серверами. Также используется для записи и получения данных в кластере ClickHouse.

Порты, используемые предустановленными ресурсами из состава OOTB

Порты открываются установщиком автоматически при установке KUMA.

Порты, используемые предустановленными ресурсами из состава OOTB:

- 7230/tcp
- 7231/tcp
- 7232/tcp
- 7233/tcp
- 7234/tcp
- 7235/tcp
- 5140/tcp
- 5140/udp
- 5141/tcp
- 5144/udp

Трафик Ядра KUMA в отказоустойчивой конфигурации

В таблице ниже указаны инициатор соединения (источник) и назначение. Номер порта на инициаторе может быть динамическим. Обратный трафик в рамках установленного соединения не должен блокироваться.

Трафик Ядра KUMA в отказоустойчивой конфигурации

Источник	Назначение	Порт назначения	Тип
Внешние сервисы KUMA	Балансировщик нагрузки	7209	TCP
Внешние сервисы KUMA	Балансировщик нагрузки	7210	TCP
Внешние сервисы KUMA	Балансировщик нагрузки	7220	TCP
Внешние сервисы KUMA	Балансировщик нагрузки	7222	TCP
Внешние сервисы KUMA	Балансировщик нагрузки	7223	TCP
Рабочий узел	Балансировщик нагрузки	6443	TCP
Рабочий узел	Балансировщик нагрузки	8132	TCP
Управляющий узел	Балансировщик нагрузки	6443	TCP
Управляющий узел	Балансировщик нагрузки	8132	TCP
Управляющий узел	Балансировщик нагрузки	9443	TCP
Рабочий узел	Внешние сервисы KUMA	В зависимости от настроек при создании сервиса.	TCP
Балансировщик нагрузки	Рабочий узел	7209	TCP
Балансировщик нагрузки	Рабочий узел	7210	TCP
Балансировщик нагрузки	Рабочий узел	7220	TCP
Балансировщик нагрузки	Рабочий узел	7222	TCP
Балансировщик нагрузки	Рабочий узел	7223	TCP
Внешние сервисы KUMA	Рабочий узел	7209	TCP
Внешние сервисы KUMA	Рабочий узел	7210	TCP
Внешние сервисы KUMA	Рабочий узел	7220	TCP
Внешние сервисы KUMA	Рабочий узел	7222	TCP
Внешние сервисы KUMA	Рабочий узел	7223	TCP
Рабочий узел	Рабочий узел	179	TCP
Рабочий узел	Рабочий узел	9500	TCP
Рабочий узел	Рабочий узел	10250	TCP
Рабочий узел	Рабочий узел	51820	UDP
Рабочий узел	Рабочий узел	51821	UDP
Управляющий узел	Рабочий узел	10250	TCP
Балансировщик нагрузки	Управляющий узел	6443	TCP
Балансировщик нагрузки	Управляющий узел	8132	TCP
Балансировщик нагрузки	Управляющий узел	9443	TCP
Рабочий узел	Управляющий узел	6443	TCP
Рабочий узел	Управляющий узел	8132	TCP
Рабочий узел	Управляющий узел	10250	TCP
Управляющий узел	Управляющий узел	2380	TCP
Управляющий узел	Управляющий узел	6443	TCP
Управляющий узел	Управляющий узел	9443	TCP
Управляющий узел	Управляющий узел	10250	TCP
Консоль управления кластером (CLI)	Балансировщик нагрузки	6443	TCP
Консоль управления кластером (CLI)	Управляющий узел	6443	TCP

Скачивание CA-сертификатов

В веб-интерфейсе KUMA вы можете скачать следующие CA-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.

  Этот сертификат вы также можете изменить, если хотите использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-консоли.

  В случае установки с сервисом Ядра KUMA в кластере Raft без использования балансировщика, вы можете скачать CA-сертификат REST API на любом узле, но защищенное соединение будет возможно только с узлом с core-1. На остальных узлах будет возвращаться ошибка. Если вы хотите заходить с одним сертификатом на все узлы кластера Raft напрямую без использования балансировщика, при генерации сертификата вы можете указать в поле Subject Alternative Names (SAN) FQDN всех узлов с сервисом Ядра KUMA в кластере Raft.

- CA-сертификат Microservice.

  Сертификат требуется для проверки подлинности при подключении источников журналов к пассивным коллекторам с использованием TLS, но без указания собственного сертификата.

Чтобы скачать CA-сертификат:

1. Откройте веб-интерфейс KUMA.

2. В левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **CA-сертификат REST API** или **CA-сертификат Microservice**, в зависимости от сертификата, который вы хотите скачать.

Сертификат сохраняется в папку загрузки, настроенную в вашем браузере.

Перевыпуск внутренних CA-сертификатов

Изменено место хранения самоподписанного CA-сертификата и механизм перевыпуска сертификата. Сертификат хранится в СУБД. Недопустимо применять прежний метод перевыпуска внутренних сертификатов через удаление сертификатов из файловой системы Ядра и перезапуск Ядра. Такой способ приведет к невозможности запустить Ядро. До завершения процесса перевыпуска сертификатов не следует подключать к Ядру новые сервисы.
После того как вы перевыпустите внутренние CA-сертификаты в разделе веб-интерфейса KUMA **Параметры** → **Другое** → **Общие** → **Перевыпустить внутренние CA-сертификаты**, необходимо остановить сервисы, удалить прежние сертификаты из директорий сервисов и вручную перезапустить все сервисы. Перевыпускать внутренние CA-сертификаты могут только пользователи с ролью Главный администратор.

Параметр **Перевыпустить внутренние CA-сертификаты** доступен только пользователю с ролью Главный администратор.

Перевыпуск сертификатов для отдельного сервиса остается прежним: в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** необходимо выбрать сервис, выбрать в контекстном меню **Сбросить сертификат** и удалить прежний сертификат в директории установки сервиса. KUMA 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.

Чтобы перевыпустить внутренние CA-сертификаты:

1. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие**, нажмите кнопку **Перевыпустить внутренние CA-сертификаты** и ознакомьтесь с отобразившимся предупреждением. Если вы принимаете решение продолжить перевыпуск сертификатов, нажмите **Да**.

   В результате будут перевыпущены CA-сертификаты для сервисов KUMA и CA-сертификат для ClickHouse. Далее вам нужно будет остановить сервисы, удалить прежние сертификаты из директорий установки сервисов, перезапустить Ядро и перезапустить остановленные сервисы, чтобы применить перевыпущенные сертификаты.

2. Подключитесь к хостам, где развернуты сервисы коллектора, коррелятора и маршрутизатора событий.

   a. Остановите все сервисы с помощью следующей команды:

   ```
   sudo systemctl stop kuma-<collector/correlator/eventRouter/metrics>-<ID сервиса>.service
   ```

   b. Удалите файлы сертификатов internal.cert и internal.key из директорий /opt/kaspersky/kuma/<тип сервиса>/<ID сервиса>/certificates с помощью следующей команды:

   ```
   sudo rm -f /opt/kaspersky/kuma/<тип сервиса>/<ID сервиса>/certificates/internal.cert
   sudo rm -f /opt/kaspersky/kuma/<тип сервиса>/<ID сервиса>/certificates/internal.key
   ```

3. Подключитесь к хостам, где развернуты сервисы хранилища.

   a. Остановите все сервисы хранилища.

   ```
   sudo systemctl stop kuma-<storage>-<ID сервиса>.service
   ```

   b. Удалите файлы сертификатов internal.cert и internal.key из директорий /opt/kaspersky/kuma/storage/<ID сервиса>/certificates.

   ```
   sudo rm -f /opt/kaspersky/kuma/storage/<ID сервиса>/certificates/internal.cert
   sudo rm -f /opt/kaspersky/kuma/storage/<ID сервиса>/certificates/internal.key
   ```

4. Удалите все сертификаты ClickHouse из директории /opt/kaspersky/kuma/clickhouse/certificates.

   ```
   sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
   sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
   ```

5. Подключитесь к хостам, где развернуты сервисы агентов.

   a. Остановите сервисы агентов Windows и агентов Linux.

   b. Удалите файлы сертификатов internal.cert и internal.key из рабочих директорий агентов.

6. Запустите Ядро KUMA, чтобы применить новые CA-сертификаты.

   - Для установки "all-in-one" и распределенной установки KUMA выполните команду:

     ```
     sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
     ```

   - Для KUMA с Ядром в кластере Kubernetes чтобы перезапустить Ядро KUMA, на любом контоллере 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
     ```

     Следует выполнять перезапуск Ядра KUMA с использованием команды, поскольку перезапуск Ядра KUMA через интерфейс KUMA влияет на перезапуск только контейнера Ядра KUMA, а не весь под целиком.

7. Перезапустите все сервисы, остановленные в ходе выполнения инструкции.

   ```
   sudo systemctl start kuma-<collector/correlator/eventRouter/storage/metrics>-< ID
   сервиса >.service
   ```

Внутренние CA-сертификаты перевыпущены и применены.

Изменение самоподписанного сертификата веб-консоли

Вы можете использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-консоли. Например, если вы хотите заменить сертификат веб-консоли с самоподписанного CA Core на сертификат, выпущенный корпоративным CA, необходимо предоставить external.cert и незашифрованный external.key в формате PEM.

В следующем примере показано, 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-консоли KUMA на сертификат external:

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).

   В результате получен сертификат external.cert и ключ external.key в формате PEM.

2. Если вы используете незашифрованный ключ external.key, убедитесь, что ключ в формате PKCS#8. Если файл ключа начинается с тега BEGIN RSA PRIVATE KEY, KUMA не примет файл ключа. В таком случае выполните конвертацию файла с помощью следующей команды:

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   После выполнения команды файл будет начинаться с тега BEGIN PRIVATE KEY и KUMA примет файл ключа.

3. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие** → **Параметры Ядра**. В блоке параметров **Внешняя TLS-пара** нажмите **Загрузить сертификат** и **Загрузить ключ** и загрузите external.cert и незашифрованный external.key в формате PEM.

4. Перезапустите KUMA:

   ```
   systemctl restart kuma-core
   ```

5. Обновите страницу или перезапустите браузер, с помощью которого вы работаете в веб-интерфейсе KUMA.

Сертификат и ключ вашей компании заменены.

Синхронизация времени на серверах

Чтобы настроить синхронизацию времени на серверах:

1. Установите chrony с помощью следующей команды:

   ```
   sudo apt install chrony
   ```

2. Настройте синхронизацию системного времени с NTP-сервером:

   a. Убедитесь, что виртуальная машина имеет доступ в интернет.

      Если доступ есть, вы можете перейти к шагу b.

      Если доступ отсутствует, отредактируйте файл `/etc/chrony.conf`, заменив значение `2.pool.ntp.org` на имя или IP-адрес внутреннего NTP-сервера вашей организации.

   b. Запустите сервис синхронизации системного времени, выполнив следующую команду:

      ```
      sudo systemctl enable --now chronyd
      ```

   c. Через несколько секунд выполните следующую команду:

      ```
      sudo timedatectl | grep 'System clock synchronized'
      ```

      Если системное время синхронизировано верно, вывод будет содержать строку System clock synchronized: yes.

Синхронизация настроена.

О файле инвентаря

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком kuma-ansible-installer с помощью инструмента Ansible и созданного вами файла инвентаря. Вы можете указать значения параметров конфигурации KUMA в файле инвентаря, а установщик использует эти значения при развертывании, обновлении и удалении решения. Файл инвентаря имеет формат YAML.

Вы можете создать файл инвентаря на основе шаблонов, включенных в поставку. Доступны следующие шаблоны:

- single.inventory.yml.template – используется для установки KUMA на одном сервере. Содержит минимальный набор параметров, оптимизированный для установки на одном устройстве, без использования кластера Kubernetes.

- distributed.inventory.yml.template – используется для первоначальной распределенной установки KUMA без использования кластера Kubernetes, расширения установки "все в одном" до распределенной и для обновления KUMA.

- expand.inventory.yml.template – используется в ряде сценариев изменения конфигурации: для добавления серверов коллекторов и серверов корреляторов, для расширения существующего кластера хранения и добавления нового кластера хранения. Если вы используете этот файл инвентаря для изменения конфигурации, установщик не останавливает сервисы во всей инфраструктуре. Установщик может останавливать только те сервисы, которые размещены на хостах, перечисленных в файле инвентаря expand.inventory.yml, если вы повторно используете файл инвентаря.

- k0s.inventory.yml.template – используется для установки или переноса KUMA в кластер Kubernetes.

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Параметры конфигурации KUMA в файле инвентаря

Файл инвентаря может содержать следующие блоки:

- `all`

- `kuma`

- `kuma_k0s`

Для каждого хоста вам нужно указать FQDN в формате `<имя хоста>.<домен>` и при необходимости IPv4-адрес или IPv6-адрес. Имя домена Ядра KUMA и его поддомены не должны начинаться с цифры.

```
Пример:
hosts:
  hostname.example.com:
    ip: 0.0.0.0
```

Блок all

В этом блоке вы можете указать переменные, которые распространяются на все хосты, указанные в файле инвентаря, включая неявно заданный localhost, на котором запущена установка. Переменные можно переопределять на уровне групп хостов или отдельных хостов.

Пример переопределения переменных в файле инвентаря

```
all:

  vars:

    ansible_connection: ssh

    deploy_to_k8s: False

    need_transfer: False

    airgap: True

    deploy_example_services: True
```

```
kuma:
  vars:
    ansible_become: true
    ansible_user: i.ivanov
    ansible_become_method: su
    ansible_ssh_private_key_file: ~/.ssh/id_rsa
  children:
    kuma_core:
      vars:
        ansible_user: p.petrov
        ansible_become_method: sudo
```

В таблице ниже приведен список возможных переменных в разделе `vars` и их описание.

Список возможных переменных в разделе vars

Переменная	Описание
`ansible_connection`	Способ подключения к целевым машинам. Возможные значения: • `ssh` – подключение к удаленным хостам по SSH. Если вы используете нестандартный порт для подключения к удаленным хостам по SSH, укажите значения переменной `ansible_port`. • `local` – подключение к удаленным хостам не производится.

Переменная	Описание

`ansible_port`	Переменная для указания нестандартного порта для подключения к удаленным хостам по SSH. Доступны следующие возможности настройки параметра `ansible_port`:
	• Если на всех хостах, перечисленных в файле инвентаря, используется один и тот же нестандартный порт, укажите значение переменной `ansible_port` в файле инвентаря в блоке `all` в секции `vars`.
	Пример файла инвентаря distributed.inventory.yml с одним нестандартным портом для всех хостов
	`all:`
	`  vars:`
	`  ansible_port: 2222`
	`  deploy_to_k8s: false`
	`  need_transfer: false`
	`  generate_etc_hosts: false`
	`  deploy_example_services: false`
	`  no_firewall_actions: false`
	`kuma:`
	`  vars:`
	`  ansible_connection: ssh`
	`  ansible_user: root`
	`  children:`
	`  kuma_core:`
	`  hosts:`
	`  kuma-core-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_collector:`
	`  hosts:`
	`  kuma-collector-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_correlator:`
	`  hosts:`
	`  kuma-correlator-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_storage:`
	`  hosts:`
	`  kuma-storage-cluster1-server1.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 1`
	`  keeper: 0`
	`  kuma-storage-cluster1-server2.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 2`
	`  keeper: 0`
	`  kuma-storage-cluster1-server3.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 2`
	`  replica: 1`
	`  keeper: 0`
	`  kuma-storage-cluster1-server4.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 2`
	`  replica: 2`
	`  keeper: 0`
	`  kuma-storage-cluster1-server5.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 1`
	`  kuma-storage-cluster1-server6.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 2`
	`  kuma-storage-cluster1-server7.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 3`
	• Если вы используете нестандартный порт для группы хостов, укажите значение переменной для группы хостов в файле инвентаря в блоке `kuma` или `kuma_k0s` в секции `vars`. Например:
	Пример файла инвентаря distributed.inventory.yml с одним нестандартным портом для группы хостов хранилища
	`all:`
	`  vars:`
	`  deploy_to_k8s: false`
	`  need_transfer: false`
	`  generate_etc_hosts: false`
	`  deploy_example_services: false`
	`  no_firewall_actions: false`

Переменная	Описание

	``yaml
	kuma:
	  vars:
	  ansible_connection: ssh
	  ansible_user: root
	  children:
	  kuma_core:
	  hosts:
	  kuma-core-1.example.com:
	  ip: 0.0.0.0
	  kuma_collector:
	  hosts:
	  kuma-collector-1.example.com:
	  ip: 0.0.0.0
	  kuma_correlator:
	  hosts:
	  kuma-correlator-1.example.com:
	  ip: 0.0.0.0
	  kuma_storage:
	  vars:
	  ansible_port: 2222
	  hosts:
	  kuma-storage-cluster1-server1.example.com:
	  ip: 0.0.0.0
	  shard: 1
	  replica: 1
	  keeper: 0
	  kuma-storage-cluster1-server2.example.com:
	  ip: 0.0.0.0
	  shard: 1
	  replica: 2
	  keeper: 0
	  kuma-storage-cluster1-server3.example.com:
	  ip: 0.0.0.0
	  shard: 2
	  replica: 1
	  keeper: 0
	  kuma-storage-cluster1-server4.example.com:
	  ip: 0.0.0.0
	  shard: 2
	  replica: 2
	  keeper: 0
	  kuma-storage-cluster1-server5.example.com:
	  ip: 0.0.0.0
	  shard: 0
	  replica: 0
	  keeper: 1
	  kuma-storage-cluster1-server6.example.com:
	  ip: 0.0.0.0
	  shard: 0
	  replica: 0
	  keeper: 2
	  kuma-storage-cluster1-server7.example.com:
	  ip: 0.0.0.0
	  shard: 0
	  replica: 0
	  keeper: 3
	``
	Пример файла инвентаря k0s.inventory.yml с одним нестандартным портом для всех хостов в секции kuma_control_plane
	``yaml
	all:
	  vars:
	  ansible_connection: ssh
	  ansible_user: root
	  deploy_to_k8s: true
	  need_transfer: false
	  generate_etc_hosts: false
	  deploy_example_services: false
	  no_firewall_actions: false
	  metrics_disk_request: 150Gi
	  core_disk_request: 100Gi
	kuma:
	  children:
	  kuma_collector:
	  hosts:
	  kuma-collector.example.com:
	  kuma_correlator:
	  hosts:
	  kuma-correlator.example.com:
	  kuma_storage:
	  hosts:
	  kuma-storage-cluster1.server1.example.com
	  kuma-storage-cluster1.server2.example.com
	  kuma-storage-cluster1.server3.example.com
	  kuma-storage-cluster1.server4.example.com
	``
	89

Переменная	Описание
	``` kuma-storage-cluster1.server5.example.com kuma-storage-cluster1.server6.example.com kuma-storage-cluster1.server7.example.com kuma_k0s: children: kuma_lb: hosts: kuma-lb.example.com: kuma_managed_lb: true kuma_control_plane_master: hosts: kuma_cpm.example.com: ansible_host: 10.0.1.10 kuma_control_plane_master_worker: kuma_control_plane: vars: ansible_port: 2222 hosts: kuma_cp2.example.com: ansible_host: 10.0.1.11 kuma_cp3.example.com: ansible_host: 10.0.1.12 kuma_control_plane_worker: kuma_worker: hosts: kuma-w1.example.com: ansible_host: 10.0.2.11 extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true" kuma-w2.example.com: ansible_host: 10.0.2.12 extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true" ``` **Пример файла инвентаря distributed.inventory.yml для отказоустойчивой установки с Ядром KUMA в кластере Raft с одним нестандартным портом для всех хостов с Ядром KUMA** ``` all: vars: deploy_to_k8s: false need_transfer: false generate_etc_hosts: false deploy_example_services: false no_firewall_actions: false kuma: vars: ansible_connection: ssh ansible_user: root children: kuma_core: hosts: kuma-core-1.example.com: ip: 0.0.0.0 raft_node_addr: "" ansible_port: 2222 kuma_core_peers: vars: ansible_port: 2222 hosts: kuma-core-2.example.com: ip: 0.0.0.0 kuma-core-3.example.com: ip: 0.0.0.0 kuma_collector: hosts: kuma-collector-1.example.com: ip: 0.0.0.0 kuma_correlator: hosts: kuma-correlator-1.example.com: ip: 0.0.0.0 kuma_storage: hosts: kuma-storage-cluster1-server1.example.com: ip: 0.0.0.0 shard: 1 replica: 1 keeper: 0 kuma-storage-cluster1-server2.example.com: ip: 0.0.0.0 shard: 1 replica: 2 keeper: 0 kuma-storage-cluster1-server3.example.com: ip: 0.0.0.0 ```

Переменная	Описание

```
            shard: 2
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server4.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server5.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 1
          kuma-storage-cluster1-server6.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 2
          kuma-storage-cluster1-server7.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 3
```

- Если вы используете отдельный нестандартный порт для каждого хоста для подключения по SSH, укажите значение переменной ansible_port для каждого хоста в файле инвентаря.

  Пример файла инвентаря distributed.inventory.yml с отдельным нестандартным портом для каждого хоста хранилища

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
    ansible_user: <пользователь из группы sudo>
    ansible_become: true
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          raft_node_addr: ""
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ansible_port: 2223
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2224
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

  Пример файла инвентаря k0s.inventory.yml с отдельным нестандартным портом для каждого хоста в группе kuma_control_plane

```
all:
```

Переменная	Описание

	``
	  vars:
	  ansible_connection: ssh
	  ansible_user: root
	  deploy_to_k8s: true
	  need_transfer: false
	  generate_etc_hosts: false
	  deploy_example_services: false
	  no_firewall_actions: false
	  metrics_disk_request: 150Gi
	  core_disk_request: 100Gi
	kuma:
	  children:
	  kuma_collector:
	  hosts:
	  kuma-collector.example.com:
	  kuma_correlator:
	  hosts:
	  kuma-correlator.example.com:
	  kuma_storage:
	  hosts:
	  kuma-storage-cluster1.server1.example.com
	  kuma-storage-cluster1.server2.example.com
	  kuma-storage-cluster1.server3.example.com
	  kuma-storage-cluster1.server4.example.com
	  kuma-storage-cluster1.server5.example.com
	  kuma-storage-cluster1.server6.example.com
	  kuma-storage-cluster1.server7.example.com
	kuma_k0s:
	  children:
	  kuma_lb:
	  hosts:
	  kuma-lb.example.com:
	  kuma_managed_lb: true
	  kuma_control_plane_master:
	  hosts:
	  kuma_cpm.example.com:
	  ansible_host: 10.0.1.10
	  kuma_control_plane_master_worker:
	  kuma_control_plane:
	  hosts:
	  kuma_cp2.example.com:
	  ansible_port: 2222
	  ansible_host: 10.0.1.11
	  kuma_cp3.example.com:
	  ansible_port: 2223
	  ansible_host: 10.0.1.12
	  kuma_control_plane_worker:
	  kuma_worker:
	  hosts:
	  kuma-w1.example.com:
	  ansible_host: 10.0.2.11
	  extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
	ingress=true,node.longhorn.io/create-default-disk=true"
	  kuma-w2.example.com:
	  ansible_host: 10.0.2.12
	  extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
	ingress=true,node.longhorn.io/create-default-disk=true"
	``
	Пример файла инвентаря distributed.inventory.yml для отказоустойчивой установки с Ядром KUMA в кластере Raft с отдельным портом для каждого хоста с Ядром KUMA
	``
	all:
	  vars:
	  deploy_to_k8s: false
	  need_transfer: false
	  generate_etc_hosts: false
	  deploy_example_services: false
	  no_firewall_actions: false
	kuma:
	  vars:
	  ansible_connection: ssh
	  ansible_user: root
	  children:
	  kuma_core:
	  hosts:
	  kuma-core-1.example.com:
	  ip: 0.0.0.0
	  raft_node_addr: ""
	  ansible_port: 2222
	  kuma_core_peers:
	  hosts:
	  kuma-core-2.example.com:
	  ip: 0.0.0.0
	  ansible_port: 2223
	  kuma-core-3.example.com:
	``
	92

Переменная	Описание
	``` ip: 0.0.0.0 ansible_port: 2224 kuma_collector: hosts: kuma-collector-1.example.com: ip: 0.0.0.0 kuma_correlator: hosts: kuma-correlator-1.example.com: ip: 0.0.0.0 kuma_storage: hosts: kuma-storage-cluster1-server1.example.com: ip: 0.0.0.0 shard: 1 replica: 1 keeper: 0 kuma-storage-cluster1-server2.example.com: ip: 0.0.0.0 shard: 1 replica: 2 keeper: 0 kuma-storage-cluster1-server3.example.com: ip: 0.0.0.0 shard: 2 replica: 1 keeper: 0 kuma-storage-cluster1-server4.example.com: ip: 0.0.0.0 shard: 2 replica: 2 keeper: 0 kuma-storage-cluster1-server5.example.com: ip: 0.0.0.0 shard: 0 replica: 0 keeper: 1 kuma-storage-cluster1-server6.example.com: ip: 0.0.0.0 shard: 0 replica: 0 keeper: 2 kuma-storage-cluster1-server7.example.com: ip: 0.0.0.0 shard: 0 replica: 0 keeper: 3 ```
`ansible_user`	Имя пользователя, от которого производится подключение к целевым машинам и установка компонентов. Если пользователь root на целевых машинах заблокирован, вам нужно использовать имя пользователя, имеющего право на подключение по SSH и повышение привилегий через su или sudo.
`ansible_become`	Переменная, определяющая, требуется ли повышать привилегии пользователя, от имени которого осуществляется установка компонентов KUMA. Возможные значения: • `true` – вам нужно указать это значение, если для переменной `ansible_user` вы не указали значение `root`. • `false`.
`ansible_become_method`	Способ повышения привилегий пользователя, от имени которого осуществляется установка компонентов KUMA. Вам нужно указать значение `su` или `sudo`, если для переменной `ansible_user` вы не указали значение `root`.
`ansible_ssh_private_key_file`	Путь к закрытому ключу в формате /<путь>/.ssh/id_rsa. Вам нужно указать эту переменную, если вы хотите указать файл ключа, отличный от файла ключа по умолчанию ~/.ssh/id_rsa.
`deploy_to_k8s`	Переменная, определяющая, требуется ли разворачивать компоненты KUMA в кластере Kubernetes. Возможные значения: • `false` – это значение указано в шаблонах файла инвентаря single.inventory.yml и distributed.inventory.yml. • `true` – это значение указано в шаблоне файла инвентаря k0s.inventory.yml. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.

Переменная	Описание
`need_transfer`	Переменная, определяющая, требуется ли переносить Ядро KUMA в новый кластер Kubernetes. Вам нужно указать эту переменную, только если для переменной `deploy_to_k8s` вы указали значение `true`. Возможные значения: • `false` – KUMA требуется установить или обновить в кластере Kubernetes. • `true` – Ядро KUMA требуется перенести в новый кластер Kubernetes. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.
`no_firewall_actions`	Переменная, определяющая, выполняет ли установщик шаги по настройке межсетевого экрана на хостах. Возможные значения: • `true` – при запуске установщик не выполняет шаги по настройке межсетевого экрана на хостах. • `false` – при запуске установщик выполняет шаги по настройке межсетевого экрана на хостах. Это значение указано во всех шаблонах файла инвентаря. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.
`generate_etc_hosts`	Переменная, определяющая, регистрируются ли машины в DNS-зоне вашей организации. Установщик автоматически дополнит файлы /etc/hosts на машинах, на которые устанавливаются компоненты KUMA, IP-адресами машин из файла инвентаря. Указанные IP-адреса должны быть уникальными. Возможные значения: • `false`. • `true`. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`. При использовании `generate_etc_hosts: true` в файле инвентаря для отказоустойчивой конфигурации нужно обязательно указать IP-адрес балансировщика в переменной `ansible_host` для хоста балансировщика в секции `kuma_lb`.
`deploy_example_services`	Переменная, определяющая, создаются ли предустановленные сервисы при установке KUMA. Вам нужно указать эту переменную, если вы хотите создать демо-сервисы независимо от файла инвентаря single/distributed/k0s. Возможные значения: • `false` – предустановленные сервисы не создаются при установке KUMA. Это значение указано во всех шаблонах файла инвентаря. • `true` – предустановленные сервисы создаются при установке KUMA. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.
`low_resources`	Переменная, определяющая, устанавливается ли KUMA в окружениях с ограниченными вычислительными ресурсами. Эта переменная отсутствует во всех шаблонах файла инвентаря. Возможные значения: • `false` – KUMA устанавливается для промышленной эксплуатации. В этом случае установщик проверяет требования рабочих узлов (процессор, ОЗУ и свободное дисковое пространство) в соответствии с аппаратными и программными требованиями. Если требования не выполняются, установка прерывается с сообщением об ошибке. • `true` – KUMA устанавливается в окружениях с ограниченными вычислительными ресурсами. В этом случае минимальный объем директории для установки Ядра KUMA на хосте составляет 4 ГБ. Ограничения для других вычислительных ресурсов отсутствуют. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.
`core_disk_request`	Переменная, позволяющая определить размер тома Ядра KUMA для установки в кластере Kubernetes. Если значение переменной не задано, то для размера тома Ядра KUMA при установке будут принятые следующие значения по умолчанию: • Если `low_resources=false`, размер тома по умолчанию - 100Gi. • Если `low_resources=true`, размер тома по умолчанию - 4Gi. Суффикс Gi обязателен для указания.
`metrics_disk_request`	Переменная, позволяющая определить размер тома сервиса Метрики для установки в кластере Kubernetes. Если значение переменной не задано, то для размера тома сервиса Метрики при установке будут приняты следующие значения по умолчанию: • Если `low_resources=false`, размер тома по умолчанию - 80Gi. • Если `low_resources=true`, размер тома по умолчанию - 4Gi. Суффикс Gi обязателен для указания.
`metrics_transfer_job_timeout`	Переменная, позволяющая определить срок ожидания копирования метрик в минутах из тома Ядра KUMA 3.4 в новый том метрик в KUMA 4.0. Значение по умолчанию: 120m. Суффикс m обязателен для указания.

Переменная	Описание
`mtu`	Переменная, позволяющая определить максимальный размер данных для передачи в одном пакете в сетевой среде без необходимости фрагментации в кластере Kubernetes. Для решения проблемы с избыточным повторением передачи пакетов или полным пропаданием связи внутри шифрованного канала мы рекомендуем указать значение параметра `mtu` меньшее, чем минимальное значение `mtu` в существующем канале связи между рабочими узлами. Если значение не задано, применяется автоматическое определение максимального размера данных на основании типов интерфейсов хостов.
`backup_timeout`	Переменная, позволяющая определить максимальное время в секундах, отведенное на создание резервной копии Ядра KUMA и отдельно на восстановление данных из резервной копии в кластере Kubernetes. Например, если вы указали значение 2700, это значит, что будет выделено 2700 секунд на создание резервной копии и 2700 секунд на восстановление из резервной копии. Если параметр не указан в файле инвентаря в секции vars, при автоматическом создании резервной копии Ядра KUMA и автоматическом восстановлении данных из резервной копии, будет принято значение по умолчанию. Значение по умолчанию: 1800 секунд. Если автоматическое создание резервной копии завершилось раньше указанного значения, скрипт обновления продолжает дальнейшую работу сразу. Изменять значение параметра в большую сторону имеет смысл, если создание резервной копии Ядра KUMA вручную занимает около 30 минут или больше.

Блок kuma

В этом блоке вы можете указать параметры компонентов KUMA, развернутых вне кластера Kubernetes. Блок `kuma` может содержать следующие разделы:

- `vars` – переменные, которые распространяются на все хосты, указанные в блоке `kuma`.
- `children` – группы параметров компонентов:
  - `kuma_core` – параметры Ядра KUMA.
    - `raft_node_addr` – адрес, который будет использоваться для кластера узлов с сервисом Ядра KUMA, должен быть публичным и известным для других узлов. После того, как Ядро KUMA было запущено в первый раз с этим адресом, адрес больше не может меняться в будущем для этого узла. Значение параметра следует указывать в следующем формате: <FQDN>:`<порт>`. Если значение параметра не указано явно, то в качестве <FQDN> по умолчанию принимается FQDN, где разворачивается Ядро KUMA, а `<порт>` - 7209. Параметр `raft_node_addr` следует задавать вместе с параметром `raft_node_listen на каждом сервере с Ядром KUMA в том случае, если DNS настроен таким образом, что сервер содержит несколько FQDN`. Необязательный параметр.
    - `raft_node_listen` – адрес, на котором узел будет слушать сообщения от соседей по кластеру. Значение параметра следует указывать в следующем формате `<IP-адрес сервера, на котором установлено Ядро KUMA в формате IPv4 или IPv6>:<порт>`. Адрес может меняться. Параметр `raft_node_listen` следует задавать вместе с параметром `raft_node_addr на каждом сервере с Ядром KUMA`. Необязательный параметр.
  - `kuma_core_peers` – параметры дополнительных Ядер KUMA. Установщик подготавливает серверы, перечисленные в группе `kuma_core_peers`, для последующей установки дополнительных сервисов Ядра KUMA. В этой группе можно указать только четное количество серверов. Если группа `kuma_core_peers` отсутствует в файле инвентаря или не заполнена, выполняется обычная процедура установки или обновления с одним Ядром KUMA. На каждом сервере в группе `kuma_core_peers` допускается установка только одного сервиса Ядра KUMA.

Использование группы kuma_core_peers при разных вариантах использования установщика

Вариант использования установщика	Группа kuma_core_peers в файле инвентаря есть	Группы kuma_core_peers в файле инвентаря нет или группа не заполнена
Установка с помощью установщика install.sh	Серверы из группы подготавливаются к запуску на них сервиса Ядра KUMA. На сервере из группы kuma_core устанавливается сервис kuma-core-00000000-0000-0000-0000-000000000000 (в веб-интерфейсе отображается как core-1). На всех серверах из группы kuma_core_peers последовательно устанавливаются и запускаются сервисы kuma-core-UID (в веб-интерфейсе отображаются как core-<FQDN>), подключаемые к сервису core-1. Все дополнительные сервисы так же подключаются к mongoDB, запущенной на сервере с core-1, поэтому mongoDB связывается со всеми IP-адресами сервера с core-1 и на межсетевом экране открывается доступ к порту 27017/tcp.	Выполняется штатная установка с одним сервисом core-1 и одним сервисом метрик на сервере из группы kuma_core.
Обновление с версии 3.4.x с помощью установщика install.sh	Серверы из группы kuma_core_peers подготавливаются к запуску сервиса Ядра KUMA. Сервисы Ядра KUMA на них не устанавливаются. Вы можете позднее создать дополнительные сервисы Ядра KUMA в веб-интерфейсе и установить их на подготовленные серверы.	Выполняется обычное обновление, прежние сервисы метрик заменяются новым, запущенным на сервере из группы kuma_core.
Расширение установки с помощью установщика expand.sh	В существующей установке можно создать или расширить кластер Raft. Для этого нужно создать файл инвентаря expand.inventory.yml, но заполнить в нем только группу kuma_core_peers. После запуска установщика expand.sh с файлом инвентаря expand.inventory.yml нужно вручную создать в веб-интерфейсе сервисы Ядра KUMA и установить их на подготовленные установщиком серверы. После расширения кластера Raft следует актуализировать группу kuma_core_peers в файле инвентаря distributed.inventory.yml на случай обновления KUMA.	Выполняется обычное расширение установки.

- `raft_node_addr` – адрес, который будет использоваться для кластера узлов с сервисом Ядра KUMA, должен быть публичным и известным для других узлов. После того, как Ядро KUMA было запущено в первый раз с этим адресом, адрес больше не может меняться в будущем для этого узла. Значение параметра следует указывать в следующем формате: <FQDN>:`<порт>`. Если значение параметра не указано явно, то в качестве <FQDN> по умолчанию принимается FQDN, где разворачивается Ядро KUMA, а `<порт>` - 7209. Параметр `raft_node_addr` следует задавать вместе с параметром `raft_node_listen` на каждом сервере с Ядром KUMA в том случае, если DNS настроен таким образом, что сервер содержит несколько FQDN. Необязательный параметр.

- `raft_node_listen` – адрес, на котором узел будет слушать сообщения от соседей по кластеру. Значение параметра следует указывать в следующем формате `<IP-адрес сервера, на котором установлено Ядро KUMA в формате IPv4 или IPv6>:<порт>`. Адрес может меняться. Параметр `raft_node_listen` следует задавать вместе с параметром `raft_node_addr на каждом сервере с Ядром KUMA`. Необязательный параметр.

- `kuma_metrics` – параметры сервиса Метрики. Вы можете указать только один хост. При переносе Ядра KUMA в кластер Kubernetes необходимо предварительно перенести сервис Метрики на один хост с Ядром KUMA при помощи установщика expand.sh и файла инвентаря expand.inventory.yml. При переносе Ядра KUMA в кластер Kubernetes выполняется проверка на наличие запущенного сервиса Метрики на этом хосте. Если сервис Метрики не найден, вернется ошибка и перенос будет прерван. При переносе Ядра KUMA в кластер Kubernetes данные метрик переносятся в кластер.

- `kuma_collector` – параметры коллекторов KUMA. Вы можете указать несколько хостов.

- `kuma_correlator` – параметры корреляторов KUMA. Вы можете указать несколько хостов.

- `kuma_storage` – параметры узлов хранилища KUMA. Вы можете указать несколько хостов, а также идентификаторы шарда, реплики и кипера для хостов с помощью следующих параметров:

  - `shard` – идентификатор шарда.

  - `replica` – идентификатор реплики.

  - `keeper` – идентификатор кипера.

  Указанные идентификаторы шарда, реплики и кипера используются, только если вы разворачиваете демо-сервисы при новой установке KUMA. В остальных случаях используются идентификаторы шарда, реплики и кипера, которые вы указали в веб-интерфейсе KUMA при [создании набора ресурсов для хранилища](#).

Блок kuma_k0s

В этом блоке вы можете указать параметры кластера Kubernetes, использование которого обеспечивает отказоустойчивость KUMA. Этот блок указан только в файле инвентаря, основанном на шаблоне файла инвентаря k0s.inventory.yml.template.

> Для тестовой и демонстрационной установки в окружениях с ограниченными вычислительными ресурсами вам нужно указать переменную `low_resources: true` в блоке `all`. В этом случае минимальный объем директории для установки ядра KUMA будет снижен до 4 ГБ и ограничения для других вычислительных ресурсов не будут указаны.

Для каждого хоста в блоке `kuma_k0s` должен быть указан уникальный FQDN и IP-адрес с помощью переменной `ansible_host`, кроме хоста в разделе `kuma_lb`. Для хоста в разделе `kuma_lb` должен быть указан только FQDN. Хосты в группах не должны повторяться.

> Для демонстрационной установки допустимо совместить контроллер с рабочим узлом. Такая конфигурация не обеспечивает отказоустойчивости Ядра KUMA и служит для демонстрации возможностей или проверки программной среды.
> Минимальная конфигурация для обеспечения отказоустойчивости составляет 3 контроллера, 2 рабочих узла и 1 балансировщик нагрузки nginx. Для промышленной эксплуатации рекомендуется использовать отдельные рабочие узлы и контроллеры. Если контроллер кластера находится под рабочей нагрузкой и под (англ. pod) с Ядром KUMA размещается на контроллере, выключение контроллера приведет к полной потере доступа к Ядру KUMA.

Блок `kuma_k0s` может содержать следующие разделы:

- `vars` – переменные, которые распространяются на все хосты, указанные в блоке `kuma`.

- `children` – параметры кластера Kubernetes, использование которого обеспечивает отказоустойчивость KUMA.

В таблице ниже приведен список возможных переменных в разделе `vars` и их описание.

Список возможных переменных в разделе `vars`

Группа переменных	Описание	
`kuma_lb`	FQDN балансировщика нагрузки. Вы можете установить балансировщик нагрузки nginx или сторонний TCP-балансировщик нагрузки. Если вы устанавливаете балансировщик нагрузки nginx, вы можете указать параметр `kuma_managed_lb = true`, чтобы автоматически настроить балансировщик нагрузки nginx при установке KUMA, открыть на хосте балансировщика нагрузки nginx необходимые сетевые порты (6443, 8132, 9443, 7209, 7210, 7220, 7222, 7223, 7226), а также выполнить перезагрузку для применения изменений. Если вы устанавливаете сторонний TCP-балансировщик нагрузки, вам нужно вручную настроить его до установки KUMA.	
`kuma_control_plane_master`	Хост, выполняющий роль главного контроллера в кластере.	Группы для указания главного контроллера. Вам нужно указать хост только для одной группы.
`kuma_control_plane_master_worker`	Хост, совмещающий роль главного контроллера и рабочего узла в кластере. Для каждого контроллера кластера, совмещенного с рабочим узлом, в файле инвентаря должен быть указан параметр `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`.	
`kuma_control_plane`	Хосты, выполняющие роль контроллера в кластере.	Группы для указания второстепенных контроллеров.
`kuma_control_plane_worker`	Хосты, совмещающие роль контроллера и рабочего узла в кластере. Для каждого контроллера кластера, совмещенного с рабочим узлом, в файле инвентаря должен быть указан параметр `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`.	
`kuma_worker`	Рабочие узлы кластера. Для каждого рабочего узла в файле инвентаря должен быть указан параметр `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`.	
`kuma_metrics`	Параметры сервиса Метрики. Вы можете указать только один хост, на котором установлено Ядро KUMA. При переносе Ядра KUMA из распределенной установки в кластер Kubernetes необходимо предварительно перенести сервис Метрики на один хост с Ядром KUMA при помощи установщика expand.sh и файла инвентаря expand.inventory.yml. При переносе Ядра KUMA в кластер Kubernetes выполняется проверка на наличие запущенного сервиса Метрики на этом хосте. Если сервис Метрики не найден, вернется ошибка и перенос будет прерван. При переносе Ядра KUMA в кластер Kubernetes данные метрик переносятся в кластер.	

`ipAutodetectionMethod`	Если на рабочих узлах кластера одновременно используется несколько сетевых интерфейсов, переменная `ipAutodetectionMethod` позволяет вам задать маску названия сетевого интерфейса, который должен использоваться для взаимодействия между рабочими узлами кластера.
	Например, если вы хотите использовать для связи между рабочими узлами кластера только сетевые интерфейсы с названием ethN (где N – это номер сетевого интерфейса), вы можете указать переменную следующим образом:
	`kuma_k0s:`
	`vars:`
	`ip_autodetection_method: "interface=eth.*"`
	В таком случае кластер будет использовать сетевой интерфейс с названием, совпадающим с маской `eth.*`.
	Если название сетевого интерфейса на каждом рабочем узле одинаково, например, eth0, вы можете указать переменную без маски:
	`kuma_k0s:`
	`vars:`
	`ip_autodetection_method: "interface=eth0"`
	Подробнее см. в документации Calico Open Source.	

Установка на одном сервере

Чтобы установить компоненты KUMA на одном сервере, выполните следующие шаги:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке KUMA.

2. Подготовьте файл инвентаря single.inventory.yml.

   Используйте шаблон файла инвентаря single.yml.template, который входит в поставку, чтобы создать файл инвентаря single.inventory.yml и описать в нем сетевую структуру компонентов решения. С помощью single.inventory.yml установщик развернет KUMA.

3. Установите решение.

   Установите решение и выполните вход в веб-интерфейс, используя учетные данные по умолчанию.

При необходимости вы можете разнести компоненты решения на разные серверы, чтобы продолжить работу в распределенной конфигурации.

Подготовка файла инвентаря single.inventory.yml

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible® и созданного пользователем *файла инвентаря* в формате YML с перечнем хостов компонентов KUMA и других параметров. Если вы хотите установить все компоненты KUMA на одном сервере, следует указать в файле инвентаря один и тот же хост для всех компонентов.

Чтобы создать файл инвентаря для установки на одном сервере:

1. Скопируйте архив с установщиком `kuma-ansible-installer-<номер версии>.tar.gz` на сервер и распакуйте его с помощью следующей команды (потребуется около 2 ГБ дискового пространства):

   ```
   sudo tar -xpf kuma-ansible-installer-<номер версии>.tar.gz
   ```

2. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

3. Скопируйте шаблон single.inventory.yml.template и создайте файл инвентаря с именем single.inventory.yml:

   ```
   cp single.inventory.yml.template single.inventory.yml
   ```

4. Отредактируйте параметры файла инвентаря single.inventory.yml.

   Если вы хотите, чтобы при установке были созданы предустановленные сервисы, присвойте параметру deploy_example_services значение true.

   ```
   deploy_example_services: true
   ```

   Предустановленные сервисы появятся только при первичной установке KUMA. При обновлении системы с помощью того же файла инвентаря предустановленные сервисы повторно созданы не будут.

5. Замените в файле инвентаря все строки `kuma.example.com` на имя хоста, на который следует установить компоненты KUMA.

Файл инвентаря создан. С его помощью можно установить KUMA на одном сервере.

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Пример файла инвентаря для установки на одном сервере

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: true
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
    ansible_user: <пользователь из группы sudo>
    ansible_become: true
    ansible_port: 2222
  children:
    kuma_core:
      hosts:
        kuma1.example.com:
    kuma_collector:
      hosts:
        kuma1.example.com
    kuma_correlator:
      hosts:
        kuma1.example.com
    kuma_storage:
      hosts:
        kuma1.example.com:
          shard: 1
          replica: 1
          keeper: 1
    kuma_metrics:
      hosts:
        kuma1.example.com
```

Установка KUMA на одном сервере

Вы можете установить все компоненты KUMA на одном сервере с помощью инструмента Ansible и файла инвентаря single.inventory.yml.

Чтобы установить KUMA на одном сервере:

1. Скачайте на сервер дистрибутив KUMA kuma-ansible-installer-<`номер сборки`>.tar.gz и распакуйте его. Архив распаковывается в директорию kuma-ansibleinstaller.

2. Войдите в директорию с распакованным установщиком.

3. В зависимости от типа активации решения, который вы планируете использовать, выберите один из вариантов:

   - Если вы планируете использовать активацию решения файлом ключа, поместите файл ключа в директорию <`директория установщика`>/roles/kuma/files/.

     Файл ключа должен иметь название license.key.

     ```
     sudo cp <файл ключа>.key <директория установщика>/roles/kuma/files/license.key
     ```

- Если вы планируете использовать активацию решения с помощью лицензионного кода, переходите к следующему пункту инструкции.

  > Активация решения с помощью лицензионного кода доступна только для KUMA 3.4 и более поздних версий. Для более ранних версий KUMA используется активация решения файлом ключа.

4. Запустите установку компонентов с использованием подготовленного файла инвентаря single.inventory.yml с помощью следующей команды:

   ```
   sudo ./install.sh single.inventory.yml
   ```

   Если для повышения привилегий требуется указать пароль, выполните следующую команду и укажите пароль по запросу:

   ```
   sudo ./install.sh single.inventory.yml --ask-become-pass
   ```

5. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, решение не будет установлено.

   В зависимости от типа активации решения результатом запуска установщика будет один из следующих вариантов:

   - Если вы планируете использовать активацию решения файлом ключа и поместили файл ключа в директорию `<директория установщика>`/roles/kuma/files/, в результате запуска установщика с файлом инвентаря single.inventory.yml будет установлено Ядро KUMA, все заданные в файле инвентаря сервисы и OOTB-ресурсы. Если в файле инвентаря был задан параметр `deploy_example_services=true`, демонстрационные сервисы будут установлены.

   - Если вы планируете использовать активацию решения с помощью лицензионного кода или планируете предоставить лицензионный файл позднее, в результате запуска установщика с файлом инвентаря single.inventory.yml будет установлено только Ядро KUMA и сервис Метрики.

     Чтобы установить сервисы, в консоли командной строки укажите лицензионный код. Затем запустите установщик postinstall.sh с файлом инвентаря single.inventory.yml.

     ```
     sudo ./postinstall.sh single.inventory.yml
     ```

     В результате будут созданы заданные сервисы. Вы можете выбрать, какие ресурсы вы хотите импортировать из репозитория.

6. По окончании установки войдите в веб-интерфейс KUMA и в строке браузера введите адрес веб-интерфейса KUMA, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса KUMA – `https://< FQDN хоста, на котором установлена KUMA >:7220`.

   Учетные данные для входа по умолчанию:
   - логин – `admin`
   - пароль – `mustB3Ch@ng3d!`

   После первого входа измените пароль учетной записи admin

Все компоненты KUMA установлены и выполнен вход в веб-интерфейс.

Мы рекомендуем сохранить файл инвентаря, который вы используете для установки решения. С помощью этого файла инвентаря можно будет дополнить систему компонентами или удалить KUMA.

Установку можно расширить до распределенной.

https://rutube.ru/video/7f45a6902afb8296f84d58b057cc8492/

Изменение имени хоста

Чтобы изменить имя хоста при установке на одном сервере:

1. Остановите все сервисы KUMA, выполнив следующую команду:

   `sudo systemctl stop kuma-<идентификатор_сервиса>.service`

2. Создайте файл восстановления с помощью следующей команды:

   `sudo touch /opt/kaspersky/kuma/core/<идентификатор_Ядра>/raft/.reset`

3. Перейдите в директорию systemd с конфигурацией сервиса Ядра KUMA и измените параметры запуска:

   - В параметре `--raft.node.addr` укажите новый FQDN узла.
   - Удалите параметр `--raft.join`, если он указан.

4. В конфигурационных файлах systemd других сервисов (коллектор, коррелятор, хранилище, маршрутизатор событий) измените значения следующих параметров:

   - В параметре `--core` укажите новое имя узла с Ядром KUMA.
   - В параметре `--advertise.fqdn` укажите новое имя машины.

5. Примените новые параметры, выполнив следующую команду:

   `sudo systemctl daemon-reload`

6. Измените имя хоста на узле:

   `sudo hostnamectl set-hostname <новое_имя_хоста>`

7. В файле /etc/hosts замените старое имя хоста на новое.

8. Перезагрузите узел, выполнив следующую команду:

   `sudo reboot`

9. После перезагрузки подключитесь к узлу под новым именем хоста.

10. Запустите сервис Ядра KUMA:

    ```
    sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
    ```

11. Проверьте, чтобы веб-интерфейс KUMA был доступен по новому имени хоста.

12. В параметрах хранилища KUMA укажите новое имя хоста.

13. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**, в списке сервисов установите флажок для необходимых сервисов и в панели инструментов или в меню (⋮) нажмите **Сбросить сертификат**.

    KUMA автоматически сгенерирует новый сертификат для каждого сервиса, для которого был сброшен сертификат. Для работающих сервисов перезапуск не требуется, новый сертификат будет применен автоматически. Если сервис был остановлен, необходимо перезапустить его, чтобы применить новый сертификат.

14. Удалите директории с сертификатами сервисов, выполнив следующие команды:

    ```
    /opt/kaspersky/kuma/< название_сервиса >/< идентификатор_сервиса >/certificates
    /opt/kaspersky/kuma/clickhouse/certificates
    ```

15. Перезапустите все сервисы KUMA:

    ```
    sudo systemctl restart kuma-< идентификатор_сервиса >.service
    ```

Узел с Ядром KUMA будет работать под новым именем хоста, а сервисы будут отображаться в разделе **Ресурсы и сервисы** → **Активные сервисы** в зеленом статусе.

Распределенная установка

Распределенная установка KUMA происходит в несколько этапов:

1. Проверка соблюдения аппаратных и программных требований, а также требований к установке KUMA.

2. Подготовка контрольной машины.

   Контрольная машина используется в процессе установки решения: на ней распаковывается и запускаются файлы установщика.

3. Подготовка целевых машин.

   На целевые машины устанавливаются компоненты решения.

4. Подготовка файла инвентаря distributed.inventory.yml.

   Создайте файл инвентаря с описанием сетевой структуры компонентов решения. С помощью этого файла инвентаря установщик развернет KUMA.

5. Установка решения.

   Установите решение и выполните вход в веб-интерфейс.

6. Создание сервисов.

   Создайте клиентскую часть сервисов в веб-интерфейсе KUMA и установите серверную часть сервисов на целевых машинах.

Сервисы KUMA следует устанавливать только после завершения установки KUMA. Мы рекомендуем устанавливать сервисы в такой последовательности: хранилище, коллекторы, корреляторы и агенты.

> При развертывании нескольких сервисов KUMA на одном хосте в процессе установки требуется указать уникальные порты для каждого сервиса с помощью параметров `--api.port <порт>`.

При необходимости вы можете изменить сертификат веб-консоли KUMA на сертификат своей компании.

[▷]

https://rutube.ru/video/a0a310d160e408015b7009e8a756ffaa/

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке решения.

2. Сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин, выполнив следующую команду:

   ```
   sudo ssh-keygen -f /root/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   Если на контрольной машине заблокирован доступ root по SSH, сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин с помощью **пользователя из группы sudo**:

   Если у пользователя нет прав sudo, добавьте пользователя в группу sudo:

   ```
   usermod -aG sudo user
   ```

   ```
   ssh-keygen -f /home/< имя пользователя из группы sudo >/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   В результате ключ будет сгенерирован и сохранен в домашней директории пользователя. Вам следует указать полный путь к ключу в файле инвентаря в значении параметра ansible_ssh_private_key_file, чтобы ключ был доступен при установке.

3. Убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

   ```
   sudo ssh-copy-id -i /root/.ssh/id_rsa root@< имя хоста целевой машины >
   ```

Если на контрольной машине заблокирован доступ root по SSH и вы хотите использовать ключ SSH из домашней директории пользователя из группы sudo, убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

```
ssh-copy-id -i /home/<имя пользователя из группы sudo>/.ssh/id_rsa <имя пользователя из группы sudo>@<имя хоста целевой машины>
```

4. Скопируйте архив с установщиком `kuma-ansible-installer-<version>.tar.gz` на контрольную машину и распакуйте его с помощью следующей команды (потребуется около 2 ГБ дискового пространства):

```
sudo tar -xpf kuma-ansible-installer-<номер версии>.tar.gz
```

Контрольная машина готова для установки KUMA.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке.

2. Установите имя хоста. Мы рекомендуем указывать FQDN. Например: kuma1.example.com.

   Имя хоста может начинаться с цифры, но для сервисов KUMA, использующих Raft, нужно использовать имя хоста, которое не начинается с цифры. Если имя хоста начинается с цифры, переименовывать сервер необязательно, достаточно настроить дополнительное имя (FQDN), начинающееся с буквы.

   Не следует изменять имя хоста, используемое KUMA после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами решения.

3. Зарегистрируйте целевую машину в DNS-зоне вашей организации для преобразования имен хостов в IP-адреса.

   Если в вашей организации не используется DNS-сервер, вы можете использовать для преобразования имен файл /etc/hosts. Содержимое файлов можно автоматически создать для каждой целевой машины при установке KUMA.

4. Чтобы получить имя хоста, которое потребуется указать при установке KUMA, выполните следующую команду и запишите результат:

   ```
   hostname -f
   ```

   Целевая машина должна быть доступна по этому имени для контрольной машины.

Целевая машина готова для установки компонентов KUMA.

Подготовка файла инвентаря distributed.inventory.yml

Чтобы создать файл инвентаря distributed.inventory.yml:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

2. Скопируйте шаблон distributed.inventory.yml.template и создайте файл инвентаря с именем distributed.inventory.yml:

```
cp distributed.inventory.yml.template distributed.inventory.yml
```

3. Отредактируйте параметры файла инвентаря distributed.inventory.yml.

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Пример файла инвентаря для Распределенной схемы установки

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
```

```
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 1
    kuma-storage-cluster1-server6.example.com:
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 2
    kuma-storage-cluster1-server7.example.com:
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 3
```

Установка KUMA в распределенной конфигурации

Установка KUMA производится помощью инструмента Ansible и YML-файла инвентаря. Установка производится с контрольной машины, при этом все компоненты KUMA устанавливаются на целевых машинах.

Чтобы установить KUMA:

1. На контрольной машине войдите в директорию с распакованным установщиком.

   ```
   cd kuma-ansible-installer
   ```

2. В зависимости от типа активации решения, который вы планируете использовать, выберите один из вариантов:

   - Для активации решения с помощью файла ключа, поместите файл ключа в директорию <папка установщика>/roles/kuma/files/.

     Файл ключа должен иметь название license.key.

     ```
     sudo cp <файл ключа>.key <папка установщика>/roles/kuma/files/license.key
     ```

   - Для активации решения с помощью кода активации, переходите к следующему пункту инструкции.

3. Запустите установку компонентов с использованием подготовленного файла инвентаря distributed.inventory.yml, находясь в директории с распакованным установщиком:

   ```
   sudo ./install.sh distributed.inventory.yml
   ```

   Если для повышения привилегий на целевой машине требуется указать пароль, выполните следующую команду и укажите пароль по запросу:

   ```
   sudo ./install.sh distributed.inventory.yml --ask-become-pass
   ```

4. Если вы хотите использовать нестандартный порт для подключения по протоколу SSH в ходе установки, выберите один из следующих вариантов:

   - Если порт одинаковый для группы хостов, укажите в файле инвентаря в группе vars.

     Пример файла инвентаря distributed.inventory.yml с одним нестандартным портом для группы хостов хранилища

     ```
     all:
       vars:
         deploy_to_k8s: false
         need_transfer: false
     ```

```
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2222
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
```

```
        keeper: 3
```

- Если для подключения к каждому хосту используется отдельный нестандартный порт, укажите порт для каждого хоста в файле инвентаря, например:

  Пример файла инвентаря distributed.inventory.yml с отдельным нестандартным портом для каждого хоста хранилища

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
    ansible_user: <пользователь из группы sudo>
    ansible_become: true
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          raft_node_addr: ""
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ansible_port: 2223
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2224
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
```

```
            replica: 0
            keeper: 3
```

5. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, решение не будет установлено.

   В зависимости от типа активации решения результатом запуска установщика будет один из следующих вариантов:

   - Если вы активируете решение с помощью файла ключа и поместили файл ключа в директорию <папка установщика>/roles/kuma/files/, в результате запуска установщика с файлом инвентаря distributed.inventory.yml будет установлено Ядро KUMA, все заданные в файле инвентаря сервисы и OOTB-ресурсы.

   - Если вы активируете решение с помощью кода активации или планируете загрузить файл ключа позднее, в результате запуска установщика с файлом инвентаря distributed.inventory.yml будет установлено только Ядро KUMA и сервис Метрики.

     Чтобы установить сервисы, в консоли командной строки укажите код активации. Затем запустите установщик postinstall.sh с файлом инвентаря distributed.inventory.yml.

     ```
     sudo ./postinstall.sh distributed.inventory.yml
     ```

     В результате будут созданы заданные сервисы. Вы можете выбрать, какие ресурсы вы хотите импортировать из репозитория.

6. По окончании установки войдите в веб-интерфейс KUMA и в строке браузера введите адрес веб-интерфейса KUMA, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса KUMA – `https://<FQDN хоста, на котором установлена KUMA>:7220`.

   Учетные данные для входа по умолчанию:

   - логин: `admin`
   - пароль: `mustB3Ch@ng3d!`

   После первого входа измените пароль учетной записи admin

Все компоненты KUMA установлены и выполнен вход в веб-интерфейс.

Мы рекомендуем сохранить файл инвентаря, который вы используете для установки решения. С помощью этого файла инвентаря можно будет дополнить систему компонентами или удалить KUMA.

Изменение имени хоста микросервисов

Чтобы изменить имя хоста на узле, на котором установлены сервисы KUMA:

1. Остановите все сервисы KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-<идентификатор_сервиса>.service
   ```

2. Перейдите в директорию сервисов /etc/systemd/system/ и в параметре `--advertise.fqdn` укажите новое имя машины.

3. Примените изменения, выполнив следующую команду:

   ```
   sudo systemctl daemon-reload
   ```

4. Измените имя хоста на узле, выполнив следующую команду:

   ```
   sudo hostnamectl set-hostname <новое_имя_хоста>
   ```

5. В файле /etc/hosts замените старое имя хоста на новое.

6. Перезагрузите узел, выполнив следующую команду:

   ```
   sudo reboot
   ```

7. После перезагрузки подключитесь к узлу под новым именем хоста.

8. В параметрах хранилища KUMA укажите новое имя хоста.

9. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**, в списке сервисов установите флажок для необходимых сервисов и в панели инструментов или в меню (⋮) нажмите **Сбросить сертификат**.

   KUMA автоматически сгенерирует новый сертификат для каждого сервиса, для которого был сброшен сертификат. Для работающих сервисов перезапуск не требуется, новый сертификат будет применен автоматически. Если сервис был остановлен, необходимо перезапустить его, чтобы применить новый сертификат.

10. Удалите директории с сертификатами сервисов, выполнив следующие команды:

    ```
    /opt/kaspersky/kuma/<название_сервиса>/<идентификатор_сервиса>/certificates
    /opt/kaspersky/kuma/clickhouse/certificates
    ```

11. Перезапустите все сервисы KUMA:

    ```
    sudo systemctl restart kuma-<идентификатор_сервиса>.service
    ```

Узел с Ядром KUMA будет работать под новым именем хоста, а сервисы отобразятся в разделе **Ресурсы и сервисы** → **Активные сервисы** в зеленом статусе.

Распределенная установка с Ядром KUMA в кластере Kubernetes

Вы можете обеспечить отказоустойчивость KUMA путем развертывания Ядра KUMA в кластере Kubernetes, а также использования внешнего балансировщика TCP-трафика.

Для установки KUMA в отказоустойчивом исполнении используется установщик из пакета kuma-ansible-installer-k8s-<номер сборки>.tar.gz и подготовленный вами файл инвентаря k0s.inventory.yml, в котором вы определите конфигурацию кластера. При новой установке в отказоустойчивой конфигурации всегда импортируются ресурсы OOTB. Вы можете выполнить установку с развертыванием демонстрационных сервисов. Для этого нужно в файле инвентаря указать параметр deploy_example_services: true.

Поместить Ядро KUMA в кластер Kubernetes можно следующими способами:

- Установить KUMA в кластере Kubernetes.
- Перенести Ядро существующей установки KUMA в кластер Kubernetes.

Минимальная конфигурация

В Kubernetes существует 2 роли узлов:

- контроллеры (control-plane) – узлы с этой ролью управляют кластером, хранят метаданные и распределяют рабочую нагрузку.
- рабочие (worker) – узлы с этой ролью несут полезную рабочую нагрузку, то есть размещают процессы KUMA.

Для выполнения установки KUMA в отказоустойчивой конфигурации вам понадобится:

- 3 выделенных контроллера;
- 2 рабочих узла;
- 1 TCP балансировщик.

Не следует использовать балансировщик в качестве контрольной машины для запуска установщика KUMA.

Для эффективной работы Ядра KUMA в Kubernetes необходимо выделить 3 обособленных узла с единственной ролью контроллера. Это позволит обеспечить отказоустойчивость самого кластера Kubernetes и гарантировать, что рабочая нагрузка - процессы KUMA и другие процессы - не повлияет на задачи, связанные с управлением кластером Kubernetes. В случае использования средств виртуализации следует убедиться, что узлы размещены на разных физических серверах и эти физические серверы не выполняют роль рабочих узлов.

В случае демонстрационной установки KUMA допустимо совмещать роли контроллера и рабочего узла. Однако при расширении установки до распределенной необходимо переустановить кластер Kubernetes целиком, выделив 3 отдельных узла с ролью контроллера и как минимум 2 узла с ролью рабочего узла. Обновление KUMA до следующих версий недоступно при наличии узлов, совмещающих роли контроллера и рабочего узла.

Дополнительные требования при развертывании Ядра в Kubernetes

Если вы планируете защитить сетевую инфраструктуру KUMA с помощью программы Kaspersky Endpoint Security for Linux, вам нужно сначала установить KUMA в кластере Kubernetes и только потом разворачивать Kaspersky Endpoint Security for Linux. При обновлении или удалении KUMA вам нужно предварительно остановить Kaspersky Endpoint Security for Linux с помощью команды:

```
systemctl stop kesl
```

При установке KUMA в отказоустойчивом варианте должны выполняться следующие требования:

- Общие требования к установке решения.
- На хостах, которые планируются под узлы кластера Kubernetes, не используются IP-адреса из следующих блоков Kubernetes:
  - serviceCIDR: 10.96.0.0/12;
  - podCIDR: 10.244.0.0/16.

Для IP-адресов из блоков исключен трафик на прокси-серверы.

- Каждый хост имеет уникальный идентификатор (/etc/machine-id).
- На хостах установлен и включен инструмент для управления межсетевым экраном firewalld или uwf для внесения правил в iptables.
- Установлен и настроен балансировщик нагрузки nginx (дополнительные сведения см. в документации балансировщика нагрузки nginx). Вы можете установить балансировщик нагрузки nginx с помощью одной из следующих команд:
  - `sudo yum install nginx` – для операционной системы Oracle Linux.
  - `sudo apt install nginx-full` – для операционной системы Astra Linux.
  - `sudo apt install nginx libnginx-mod-stream` – для операционной системы Ubuntu.
  - `sudo yum install nginx nginx-all-modules` – для операционной системы РЕД ОС.

Если вы хотите, чтобы балансировщик нагрузки nginx был настроен автоматически в процессе установки KUMA, установите балансировщик нагрузки nginx и откройте к нему доступ по SSH так же, как для хостов кластера Kubernetes.

Пример автоматически созданной конфигурации nginx

Установщик создает файл конфигурации `/etc/nginx/kuma_nginx_lb.conf`, пример содержимого которого приведен ниже. Секции `upstream` формируются динамически и содержат IP-адреса контроллеров кластера Kubernetes (в примере – 10.0.0.2-4 в секциях `upstream kubeAPI_backend`, `upstream konnectivity_backend`, `controllerJoinAPI_backend`) и IP-адреса рабочих узлов (в примере 10.0.1.2-3), для которых в файле инвентаря в переменной `extra_args` содержится значение `"kaspersky.com/kuma-ingress=true"`.

В конец файла `/etc/nginx/nginx.conf` дописывается строка `"include /etc/nginx/kuma_nginx_lb.conf;"`, позволяющая применить сформированный файл конфигурации. При большом количестве активных сервисов и пользователей может понадобиться увеличить лимит открытых файлов в параметрах `nginx.conf`.

Пример файла конфигурации:

```
# Ansible managed
#
# LB KUMA cluster
#

stream {
    server {
        listen          6443;
        proxy_pass      kubeAPI_backend;
    }
    server {
        listen          8132;
        proxy_pass      konnectivity_backend;
    }
    server {
        listen          9443;
        proxy_pass      controllerJoinAPI_backend;
    }
    server {
        listen          7209;
        proxy_pass      kuma-core-hierarchy_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7210;
```

```
        proxy_pass      kuma-core-services_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7220;
        proxy_pass      kuma-core-ui_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7222;
        proxy_pass      kuma-core-cybertrace_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7223;
        proxy_pass      kuma-core-rest_backend;
        proxy_timeout   86400s;
    }
    upstream kubeAPI_backend {
        server 10.0.0.2:6443;
        server 10.0.0.3:6443;
        server 10.0.0.4:6443;
    }
    upstream konnectivity_backend {
        server 10.0.0.2:8132;
        server 10.0.0.3:8132;
        server 10.0.0.4:8132;
    }
    upstream controllerJoinAPI_backend {
        server 10.0.0.2:9443;
        server 10.0.0.3:9443;
        server 10.0.0.4:9443;
    }
    upstream kuma-core-hierarchy_backend {
        server 10.0.1.2:7209;
        server 10.0.1.3:7209;
    }
    upstream kuma-core-services_backend {
        server 10.0.1.2:7210;
        server 10.0.1.3:7210;
    }
    upstream kuma-core-ui_backend {
        server 10.0.1.2:7220;
        server 10.0.1.3:7220;
    }
    upstream kuma-core-cybertrace_backend {
        server 10.0.1.2:7222;
        server 10.0.1.3:7222;
    }
    upstream kuma-core-rest_backend {
        server 10.0.1.2:7223;
        server 10.0.1.3:7223;
    }
 worker_rlimit_nofile 1000000;
 events {
worker_connections 20000;
}
# worker_rlimit_nofile – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих
процессов. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections – максимальное число соединений, которые одновременно может открыть рабочий процесс.
```

- На сервере балансировщика нагрузки nginx добавлен ключ доступа с устройства, с которого осуществляется установка KUMA.
- На сервере балансировщика нагрузки nginx в операционной системе не включен модуль SELinux.
- На хостах установлены пакеты tar, systemctl.

При установке KUMA автоматически проверяется соответствие хостов следующим аппаратным требованиям:

- Количество ядер CPU (потоков) – 12 или больше.
- ОЗУ – 22528 МБ или больше.

- Объем свободного пространства на диске в разделе /opt/ – 1000 ГБ или больше.
- Если производится первичная установка, в /var/lib/ должно быть не менее 32GB свободного места. Если установка кластера на этот узел ранее уже проводилась, размер требуемого свободного пространства уменьшается на размер директории /var/lib/k0s.

Если условия не выполняются, установка прерывается. Проверку условий при установке для демонстрации можно выключить, указав в файле инвентаря переменную `low_resources: true`.

Дополнительные требования при установке на операционной системе Astra Linux или Ubuntu

На машинах, предназначенных для развертывания кластера Kubernetes, установлены следующие пакеты:

- open-iscsi;
- wireguard;
- wireguard-tools.

Вы можете установить пакеты с помощью команды:

```
sudo apt install open-iscsi wireguard wireguard-tools
```

Дополнительные требования при установке на операционной системе Oracle Linux, РЕД ОС и на операционных системах Red Hat Enterprise Linux

На машинах, предназначенных для развертывания кластера Kubernetes, установлены следующие пакеты:

- iscsi-initiator-utils;
- wireguard-tools.

Перед установкой пакетов на операционной системе Oracle Linux вам нужно добавить репозиторий EPEL в качестве источника с помощью одной из следующих команд:

- `sudo yum install oracle-epel-release-el8` - для операционной системы Oracle Linux 8.
- `sudo yum install oracle-epel-release-el9` - для операционной системы Oracle Linux 9.

Вы можете установить пакеты с помощью команды:

```
sudo yum install iscsi-initiator-utils wireguard-tools
```

Установка KUMA в кластере Kubernetes

Распределенная установка KUMA происходит в несколько этапов:

1. Проверка соблюдения аппаратных и программных требований, а также требований к установке KUMA.

2. Подготовка контрольной машины.

   Контрольная машина используется в процессе установки решения: на ней распаковывается и запускаются файлы установщика.

3. Подготовка целевых машин.

   На целевые машины устанавливаются компоненты решения.

4. Подготовка файла инвентаря k0s.inventory.yml.

   Создайте файл инвентаря с описанием сетевой структуры компонентов решения. С помощью этого файла инвентаря установщик развернет KUMA.

5. Установка решения.

   Установите решение и войдите в веб-интерфейс.

6. Создание сервисов.

   Создайте клиентскую часть сервисов в веб-интерфейсе KUMA и установите серверную часть сервисов на целевых машинах.

   Сервисы KUMA следует устанавливать только после завершения установки KUMA. Мы рекомендуем устанавливать сервисы в такой последовательности: хранилище, коллекторы, корреляторы и агенты.

   > При развертывании нескольких сервисов KUMA на одном хосте в процессе установки требуется указать уникальные порты для каждого сервиса с помощью параметров `--api.port <порт>`.

При необходимости вы можете изменить сертификат веб-консоли KUMA на сертификат своей компании.

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке решения.

2. Сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин, выполнив следующую команду:

   ```
   sudo ssh-keygen -f /root/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   Если на контрольной машине заблокирован доступ root по SSH, сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин с помощью **пользователя из группы sudo**:

   Если у пользователя нет прав sudo, добавьте пользователя в группу sudo:

   ```
   usermod -aG sudo user
   ```

```
ssh-keygen -f /home/< имя пользователя из группы sudo >/.ssh/id_rsa -N "" -C kuma-ansible-installer
```

В результате ключ будет сгенерирован и сохранен в домашней директории пользователя. Вам следует указать полный путь к ключу в файле инвентаря в значении параметра ansible_ssh_private_key_file, чтобы ключ был доступен при установке.

3. Убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

```
sudo ssh-copy-id -i /root/.ssh/id_rsa root@< имя хоста целевой машины >
```

Если на контрольной машине заблокирован доступ root по SSH и вы хотите использовать ключ SSH из домашней директории пользователя из группы sudo, убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

```
ssh-copy-id -i /home/< имя пользователя из группы sudo >/.ssh/id_rsa < имя пользователя из группы sudo >@< имя хоста целевой машины >
```

4. Скопируйте архив с установщиком из пакета `kuma-ansible-installer-k8s-< номер версии >.tar.gz` на контрольную машину и распакуйте его с помощью следующей команды:

```
sudo tar -xpf kuma-ansible-installer-k8s-< номер версии >.tar.gz
```

Контрольная машина готова для установки KUMA.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке.

2. Установите имя хоста. Мы рекомендуем указывать FQDN. Например: kuma1.example.com.

   Не следует изменять имя хоста KUMA после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами решения.

3. Зарегистрируйте целевую машину в DNS-зоне вашей организации для преобразования имен хостов в IP-адреса.

   Вариант с использованием файла /etc/hosts не применим для развертывания Ядра в Kubernetes.

4. Чтобы получить имя хоста, которое потребуется указать при установке KUMA, выполните следующую команду и запишите результат:

```
hostname -f
```

   Целевая машина должна быть доступна по этому имени для контрольной машины.

Целевая машина готова для установки компонентов KUMA.

Подготовка файла инвентаря k0s.inventory.yml

Чтобы создать файл инвентаря k0s.inventory.yml:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

```
cd kuma-ansible-installer-ha
```

2. Скопируйте шаблон k0s.inventory.yml.template и создайте файл инвентаря с именем k0s.inventory.yml:

```
cp k0s.inventory.yml.template k0s.inventory.yml
```

3. Отредактируйте параметры файла инвентаря k0s.inventory.yml.

Пример файла инвентаря для установки с Ядром KUMA в кластере Kubernetes с 3 контроллерами, 2 рабочими узлами и 1 балансировщиком

```
all:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
          ansible_port: 2221
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2223
      hosts:
        kuma-storage-cluster1.server1.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server2.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server3.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server4.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server5.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server6.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server7.example.com:
          ip: 0.0.0.0
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          ip: 0.0.0.0
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp2.example.com:
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
        kuma-w1.example.com:
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
```

```
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

Для такой конфигурации следует указать параметры need_transfer: false, deploy_example_services: false, в разделе kuma_storage перечислить серверы для кластера хранения. Роли шарда, реплики и кипера вы сможете назначить указанным в инвентаре серверам в веб-интерфейсе KUMA после завершения установки.

Пример файла инвентаря для переноса Ядра в кластер Kubernetes из распределенной установки для обеспечения отказоустойчивости

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: true
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
    kuma_storage:
      hosts:
        kuma-storage-cluster1.server1.example.com
        kuma-storage-cluster1.server2.example.com
        kuma-storage-cluster1.server3.example.com
        kuma-storage-cluster1.server4.example.com
        kuma-storage-cluster1.server5.example.com
        kuma-storage-cluster1.server6.example.com
        kuma-storage-cluster1.server7.example.com
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp2.example.com:
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
```

```
        kuma-w1.example.com:
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались в файле distributed.inventory.yml при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до следующих версий, или при новой установке решения. В файле инвентаря k0s.inventory.yml необходимо указать параметры deploy_to_k8s: true, need_transfer:true, deploy_example_services: false.

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Установка с Ядром KUMA в кластере Kubernetes

Установка KUMA производится помощью инструмента Ansible и файла инвентаря k0s.inventory.yml. Установка производится с контрольной машины, при этом все компоненты KUMA устанавливаются на целевых машинах.

Чтобы установить KUMA:

1. На контрольной машине войдите в директорию с распакованным установщиком:

   ```
   cd kuma-ansible-installer-ha
   ```

2. В зависимости от типа активации решения, который вы планируете использовать, выберите один из вариантов:

   - Для активации решения с помощью файла ключа, поместите файл ключа в директорию <папка установщика>/roles/kuma/files/.

     Файл ключа должен иметь название license.key.

     ```
     sudo cp <файл ключа>.key <папка установщика>/roles/kuma/files/license.key
     ```

   - Для активации решения с помощью кода активации, переходите к следующему пункту инструкции.

3. Запустите установку компонентов с использованием подготовленного файла инвентаря distributed.inventory.yml, находясь в папке с распакованным установщиком:

   ```
   sudo ./install.sh k0s.inventory.yml
   ```

   Если для повышения привилегий на целевой машине требуется указать пароль, выполните следующую команду и укажите пароль по запросу:

   ```
   sudo ./install.sh k0s.inventory.yml --ask-become-pass
   ```

4. Если вы хотите использовать нестандартный порт для подключения по протоколу SSH в ходе установки, выберите один из следующих вариантов:

   - Если порт одинаковый для группы хостов, укажите порт в файле инвентаря в группе vars.

     Пример файла инвентаря k0s.inventory.yml с одним нестандартным портом для всех хостов в секции kuma_control_plane

     ```
     all:
       vars:
         ansible_connection: ssh
         ansible_user: root
         deploy_to_k8s: true
         need_transfer: false
         generate_etc_hosts: false
         deploy_example_services: false
         no_firewall_actions: false
         metrics_disk_request: 150Gi
         core_disk_request: 100Gi
     kuma:
       children:
         kuma_collector:
           hosts:
             kuma-collector.example.com:
         kuma_correlator:
           hosts:
             kuma-correlator.example.com:
         kuma_storage:
           hosts:
             kuma-storage-cluster1.server1.example.com
             kuma-storage-cluster1.server2.example.com
             kuma-storage-cluster1.server3.example.com
             kuma-storage-cluster1.server4.example.com
             kuma-storage-cluster1.server5.example.com
             kuma-storage-cluster1.server6.example.com
             kuma-storage-cluster1.server7.example.com
     kuma_k0s:
       children:
         kuma_lb:
           hosts:
             kuma-lb.example.com:
               kuma_managed_lb: true
         kuma_control_plane_master:
           hosts:
             kuma_cpm.example.com:
               ansible_host: 10.0.1.10
         kuma_control_plane_master_worker:
         kuma_control_plane:
           vars:
             ansible_port: 2222
           hosts:
             kuma_cp2.example.com:
               ansible_host: 10.0.1.11
             kuma_cp3.example.com:
               ansible_host: 10.0.1.12
         kuma_control_plane_worker:
         kuma_worker:
           hosts:
             kuma-w1.example.com:
     ```

```
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

- Если для подключения к каждому хосту используется отдельный нестандартный порт, укажите порт для каждого хоста в файле инвентаря.

  Пример файла инвентаря k0s.inventory.yml с отдельным нестандартным портом для каждого хоста в группе kuma_control_plane

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
    kuma_storage:
      hosts:
        kuma-storage-cluster1.server1.example.com
        kuma-storage-cluster1.server2.example.com
        kuma-storage-cluster1.server3.example.com
        kuma-storage-cluster1.server4.example.com
        kuma-storage-cluster1.server5.example.com
        kuma-storage-cluster1.server6.example.com
        kuma-storage-cluster1.server7.example.com
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp2.example.com:
          ansible_port: 2222
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
```

```
          ansible_port: 2223
          ansible_host: 10.0.1.12
      kuma_control_plane_worker:
      kuma_worker:
        hosts:
          kuma-w1.example.com:
            ansible_host: 10.0.2.11
            extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
          kuma-w2.example.com:
            ansible_host: 10.0.2.12
            extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

5. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, решение не будет установлено.

   В зависимости от типа активации решения результатом запуска установщика будет один из следующих вариантов:

   - Если вы активируете решение с помощью файла ключа и поместили файл ключа в директорию <папка установщика>/roles/kuma/files/, в результате запуска установщика с файлом инвентаря k0s.inventory.yml будет установлено Ядро KUMA, все заданные в файле инвентаря сервисы и OOTB-ресурсы.

   - Если вы активируете решение с помощью кода активации или планируете загрузить файл ключа позднее, в результате запуска установщика с файлом инвентаря k0s.inventory.yml будет установлено только Ядро KUMA.

     Чтобы установить сервисы, в консоли командной строки укажите код активации. Затем запустите установщик postinstall.sh с файлом инвентаря k0s.inventory.yml.

     ```
     sudo ./postinstall.sh k0s.inventory.yml
     ```

     В результате будут созданы заданные сервисы. Вы можете выбрать, какие ресурсы вы хотите импортировать из репозитория.

6. По окончании установки войдите в веб-интерфейс KUMA и в строке браузера введите адрес веб-интерфейса KUMA, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса KUMA – `https://<FQDN балансировщика нагрузки nginx>:7220`.

   Учетные данные для входа по умолчанию:

   - логин: `admin`
   - пароль: `mustB3Ch@ng3d!`

   После первого входа измените пароль учетной записи admin

Все компоненты KUMA установлены и выполнен вход в веб-интерфейс.

Мы рекомендуем сохранить файл инвентаря, который вы используете для установки решения. С помощью этого файла инвентаря можно будет дополнить систему компонентами или удалить KUMA.

Перенос Ядра KUMA в новый кластер Kubernetes

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.

- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Доступность Ядра KUMA при различных сценариях

Доступность Ядра KUMA при различных сценариях:

- **Выход из строя или отключение от сети рабочего узла, на котором развернут сервис Ядра KUMA.**

  Доступ к веб-интерфейсу KUMA пропадает. Через 6 минут Kubernetes инициирует перенос контейнера с Ядром на работающий узел кластера. После завершения развертывания, которое занимает менее одной минуты, веб-интерфейс KUMA снова доступен по URL, в которых используются FQDN балансировщика. Чтобы определить, на каком из хостов работает Ядро, в терминале одного из контроллеров выполните команду:

  ```
  k0s kubectl get pod -n kuma -o wide
  ```

  Когда вышедший из строя рабочий узел или доступ к нему восстанавливается, контейнер с Ядром не переносится с текущего рабочего узла. Восстановленный узел может участвовать в репликации дискового тома сервиса Ядра.

- **Выход из строя или отключение от сети рабочего узла с репликой диска Ядра KUMA, на котором в этот момент не развернут сервис Ядра.**

  Доступ к веб-интерфейсу KUMA не пропадает по URL, в которых используется FQDN балансировщика. Сетевое хранилище создает реплику работающего дискового тома Ядра на других работающих узлах. При доступе к KUMA через URL с FQDN работающих узлов перерыва также не возникает.

- **Потеря доступности одного или нескольких контроллеров кластера при сохранении кворума.**

  Рабочие узлы работают в обычном режиме. Перерыва в доступе к KUMA не возникает. Выход из строя контроллеров кластера, при котором кворум не обеспечивается оставшимися в работе контроллерами, ведет к потере управления кластером.

Соответствие количества используемых машин для обеспечения отказоустойчивости

Количество контроллеров при установке кластера	Минимальное количество контроллеров, необходимое для работы кластера (кворум)	Возможное количество неработающих контроллеров
1	1	0
2	2	0
3	2	1
4	3	1
5	3	2

Количество контроллеров при установке кластера	Минимальное количество контроллеров, необходимое для работы кластера (кворум)	Возможное количество неработающих контроллеров
6	4	2
7	4	3
8	5	3
9	5	4

- **Одновременный выход из строя всех контроллеров кластера Kubernetes.**

  Кластером невозможно управлять, из-за чего его работоспособность будет нарушена.

- **Одновременная потеря доступности всех рабочих узлов кластера с репликами тома Ядра и подом Ядра.**

  Доступ к веб-интерфейсу KUMA пропадает. Если утеряны все реплики, будет потеряна информация.

Управление Kubernetes и доступ к KUMA

При установке KUMA в отказоустойчивом варианте, в директории установщика создается файл artifacts/k0s-kubeconfig.yml, содержащий реквизиты, необходимые для подключения к созданному кластеру Kubernetes. Такой же файл создается на основном контроллере в домашней директории пользователя, заданного в файле инвентаря как ansible_user.

Для обеспечения возможности мониторинга и управления кластером Kubernetes файл k0s-kubeconfig.yml необходимо сохранить в месте, доступном для администраторов кластера. Доступ к файлу следует ограничить.

Управление кластером Kubernetes

Для мониторинга и управления кластером можно использовать программу k0s, устанавливаемую на все узлы кластера при развертывании KUMA. Например, для просмотра нагрузки на рабочие узлы можно использовать команду:

```
k0s kubectl top nodes
```

Доступ к Ядру KUMA

Доступ к Ядру KUMA осуществляется по URL `https://<FQDN рабочего узла>:<порт рабочего узла>`. Доступные порты: 7209, 7210, 7220, 7222, 7223. По умолчанию для подключения к веб-интерфейсу Ядра KUMA используется порт 7220. Доступ может осуществляться через любой рабочий узел, в параметре `extra_args` которого содержится значение `kaspersky.com/kuma-ingress=true`.

Одновременно войти в веб-интерфейс KUMA на нескольких рабочих узлах с помощью одинаковых учетных данных невозможно: активным остается только подключение, установленное последним.

В случае использования внешнего балансировщика нагрузки в конфигурации кластера Kubernetes с обеспечением отказоустойчивости доступ к портам Ядра KUMA осуществляется через FQDN балансировщика.

Часовой пояс в кластере Kubernetes

Внутри кластера Kubernetes всегда используется часовой пояс UTC+0, поэтому при обращении с данными, созданными Ядром KUMA, развернутом в отказоустойчивом варианте, следует учитывать эту разницу во времени:

- В событиях аудита в поле `DeviceTimeZone` будет указан часовой пояс UTC+0.
- В сформированных отчетах пользователь будет видеть разницу между временем формирования отчета и временем браузера.
- В панели мониторинга пользователь будет видеть разницу между временем в виджете (отображается время браузера пользователя) и временем в выгрузке данных виджета в CSV-файле (отображается время внутри кластера Kubernetes).

Обслуживание хостов в кластере Kubernetes

В процессе работы периодически возникает необходимость перезагрузки, установки обновлений или обновления операционной системы на рабочих узлах и контроллерах кластера Kubernetes. В этой статье описывается порядок обслуживания хостов, позволяющий минимизировать простой Ядра KUMA в отказоустойчивой конфигурации.

Перед вводом хостов в обслуживание необходимо создать резервную копию Ядра KUMA.

Обслуживание контроллеров

Контроллеры кластера требуется обслуживать по одному. Перед началом обслуживания контроллера дополнительные действия не требуются. После выполнения обслуживания или обновления следует убедиться, что служба контроллера успешно запущена, проверив состояние сервиса с помощью следующих команд:

```
sudo systemctl status k0scontroller
```

```
sudo k0s status
```

После восстановления обслуживаемого контроллера можно выполнять обслуживание следующего контроллера. При поочередном обслуживании контроллеров перерывов доступа к Ядру KUMA не возникает.

Обслуживание рабочих узлов

Рабочие узлы кластера требуется выводить в обслуживание по одному.

Чтобы выполнить обслуживание рабочих узлов:

1. Получите имена и текущее состояние рабочих узлов, выполнив на любом контроллере следующую команду:

```
sudo k0s kubectl get nodes
```

Все рабочие узлы должны быть в состоянии `ready`, иначе вывод из работы последующих узлов может привести к недоступности Ядра KUMA.

2. Перед обновлением рабочего узла сначала необходимо запретить размещение подов на этом узле. Чтобы запретить размещение подов, на любом контроллере выполните следующую команду:

   ```
   sudo k0s kubectl cordon <имя_рабочего_узла>
   ```

   После этого в выводе команды `sudo k0s kubectl get nodes` узел будет отображаться в статусе `Ready,SchedulingDisabled`.

3. Получите имя рабочего узла, на котором выполняется Ядро KUMA, выполнив на любом контроллере следующую команду:

   ```
   sudo k0s kubectl get pods -n kuma -o wide
   ```

4. Если Ядро KUMA работает на узле, для которого выполняется обслуживание, перезапустите развертывание Ядра KUMA, чтобы Ядро KUMA переехало на другой рабочий узел, и дождитесь успешного запуска Ядра KUMA на другом рабочем узле. Чтобы перезапустить развертывание Ядра KUMA, выполните следующую команду:

   ```
   sudo k0s kubectl rollout restart deployment core-deployment -n kuma
   ```

   > Во время переноса Ядра KUMA на другой рабочий узел доступ к Ядру KUMA будет приостановлен примерно на 10 минут.

5. Проверьте состояние Ядра KUMA, повторно выполнив следующую команду:

   ```
   sudo k0s kubectl get pods -n kuma -o wide
   ```

   Статус пода должен быть `Running`, имя рабочего узла в столбце `NODE` должно измениться.

6. Остановите сервис k0sworker на выводимом рабочем узле с помощью следующей команды:

   ```
   sudo k0s stop
   ```

7. Обновите операционную систему.

8. Запустите сервис k0s на рабочем узле с помощью следующей команды:

   ```
   sudo k0s start
   ```

9. Убедитесь, что сервис k0s успешно запущен, выполнив на рабочем узле следующие команды:

   ```
   sudo systemctl status k0sworker
   ```

   ```
   sudo k0s status
   ```

   k0sworker.service должен быть в состоянии `active (running)`.

   k0s status должен вернуть `Status: Running`.

10. Разрешите запускать поды на обновленном рабочем узле, выполнив на любом контроллере следующую команду:

    ```
    sudo k0s kubectl uncordon <имя_рабочего_узла>
    ```

11. Убедитесь, что рабочий узел в кластере доступен, выполнив на любом контроллере следующую команду:

    ```
    sudo k0s kubectl get nodes
    ```

    У обновленного рабочего узла должен быть статус `ready`.

12. После возвращения рабочего узла в кластер убедитесь, что все реплики томов восстановлены и доступны. Чтобы просмотреть состояние тома, выполните следующую команду:

    ```
    sudo k0s kubectl get volume -n longhorn-system -o json | jq
    '.items[0].status.robustness'
    ```

    Статус должен быть `healthy`. Если статус `degraded`, то одна из реплик недоступна или пересобирается.

13. Если требуется отслеживать процесс пересборки тома, выполните следующую команду:

    ```
    sudo k0s kubectl get engine -n longhorn-system -o json | jq
    '.items[0].status.rebuildStatus'
    ```

14. Если требуется просмотреть текущее состояние реплик, выполните следующую команду:

    ```
    sudo k0s kubectl get replicas -n longhorn-system
    ```

    Все реплики должны быть в статусе `running`.

Обслуживание рабочего узла выполнено. Если обслуживаемый рабочий узел готов и том Ядра KUMA находится в статусе `healthy`, вы можете переходить к обслуживанию следующего рабочего узла.

Обслуживание балансировщика трафика

Обслуживание балансировщика всегда связано с перерывом доступа к Ядру KUMA как со стороны пользователей, так и со стороны сервисов KUMA. На время выключения балансировщика становится невозможен перенос пода с Ядром KUMA с одного рабочего узла на другой.

Если планируется длительный простой основного балансировщика или существенные обновления, мы рекомендуем сделать следующее:

1. Подготовить резервный балансировщик со всеми необходимыми обновлениями, продублировать конфигурацию nginx или другого используемого балансировщика трафика с основного балансировщика на резервный. Для Nginx, настраиваемого установщиком KUMA, это файлы /etc/nginx/nginx.conf и /etc/nginx/kuma_nginx_lb.conf. FQDN резервного балансировщика должен совпадать с FQDN основного балансировщика. Необходимо убедиться, что сервис балансировщика успешно запущен и правила межсетевого экрана, примененные к основному балансировщику, применимы и к резервному балансировщику.

2. Переключить трафик на резервный балансировщик, изменив IP-адрес резервного балансировщика на IP-адрес основного балансировщика. На основном балансировщике IP-адрес должен быть временно изменен на другой IP-адрес, чтобы не было конфликта IP-адресов. Убедитесь, что Ядро KUMA на резервном балансировщике работает штатно.

   > В момент переключения трафика текущие сессии могут прерваться. Если наблюдаются неполадки, вы можете указать прежние IP-адреса и продолжить работу на основном балансировщике в прежней конфигурации.

3. Произвести необходимые работы на основном балансировщике трафика.

4. Произвести обратную смену IP-адресов на основном и резервном балансировщиках.

5. Убедиться, что Ядро KUMA на обновленном основном балансировщике работает штатно.

Последний шаг может не понадобится, если нет технической необходимости в возврате в эксплуатацию бывшего основного балансировщика, то есть производится однократная замена балансировщика на обновленный хост.

Поскольку требования к ресурсам балансировщика трафика минимальны, мы рекомендуем иметь резервный клон виртуальной машины с балансировщиком для быстрого восстановления доступа к Ядру KUMA в случае проблем с основной виртуальной машиной.

Восстановление кластера Kubernetes

В этом разделе описаны альтернативы использованию снимков виртуальных машин узлов кластера как части плана восстановления после сбоев.

Обязательным требованием для восстановления является наличие актуальной резервной копии Ядра KUMA. Также мы рекомендуем сохранять используемую конфигурацию балансировщика трафика.

Составляющие части кластера Kubernetes и использование снимков их виртуальных машин

Балансировщик трафика

После первоначальной настройки балансировщик трафика представляет собой хост без сохранения состояния. Для сохранения его состояния допускается сделать снимок виртуальной машины в любое время после установки актуальной версии KUMA. Восстановление виртуальной машины из снимка возможно в любой момент, если версия KUMA на момент создания снимка совпадает с текущей версией KUMA. Если версии различаются, может потребоваться корректировка файла конфигурации балансировщика трафика с учетом изменений в перечне обслуживаемых портов.

Ограничения:

- В момент создания снимка виртуальной машины возможны разрывы текущих подключений в зависимости от типа гипервизора.
- При восстановлении из снимка происходит разрыв текущих подключений.
- На момент восстановления виртуальной машины из снимка и до установки новых подключений ядро KUMA будет недоступно.

Контроллер кластера

Контроллеры выполняют управление кластером, и в процессе эксплуатации кластера всегда должен обеспечиваться кворум контроллеров.

Допустимо кратковременное выключение контроллера при сохранении общего кворума. Допустимо поочередное создание снимков виртуальной машины контроллеров. Главное условие: если операция снятия снимка вызывает прерывание работы сервисов k0s в зависимости от гипервизора, между выполнением снимков должно обеспечиваться время на восстановление консенсуса и синхронизацию базы etcd кластера.

Ограничения:

- Восстановление одного или нескольких контроллеров из снимка виртуальной машины при работающем кластере приведет к непредсказуемым результатам.
- Использование снимка виртуальной машины контроллера может применяться только для восстановления виртуальной машины перед полным удалением кластера Ядра KUMA, последующей полной переустановкой Ядра KUMA и восстановлением его из резервной копии.

Рабочий узел кластера

На рабочих узлах кластера исполняется Ядро KUMA и хранятся реплики тома постоянного хранения, используемого сервисами Ядра KUMA. Создание снимков виртуальной машины оказывает негативное влияние на состояние тома хранения: от появления ошибок в реплике с автоматическим пересозданием реплики до возникновения ошибок в файловой системе, требующих полного отключения тома с остановкой подов Ядра KUMA. Последствия зависят от типа гипервизора, операционной системы виртуальной машины, состояния всех реплик и интенсивности дисковых операций в момент создания снимка.

Ограничения:

Восстановление рабочего узла из снимка виртуальной машины при работающем кластере может привести к выходу кластера из строя. Даже использование снимка рабочего узла, временно выведенного из эксплуатации, не обеспечивает возможности последующего возврата этого узла в кластер после восстановления виртуальной машины. Полезны могут быть снимки рабочих узлов, созданные непосредственно перед установкой Ядра KUMA. Использование таких снимков упростит подготовку к переустановке Ядра KUMA при восстановлении.

Сценарии сбоев

Временная недоступность отдельных компонентов кластера

Если отдельные компоненты кластера временно недоступны, например, из-за временного отключения питания сервера, сетевой недоступности или сбоя, потребовавшего перезагрузки сервера или виртуальной машины, для восстановления не требуется пересоздание виртуальных машин или замены серверов. Доступность Ядра KUMA в этом случае определяется набором оставшихся в работе компонентов. В этот же сценарий входят сбои на сервере или виртуальной машине, которые не требуют переустановки операционной системы и которые можно оперативно устранить заменой отдельных частей или изменением конфигурации ПО.

После восстановления работы и доступности всех компонентов работоспособность кластера восстанавливается автоматически, но некоторое время выполняются переходные операции, такие как синхронизация реплик тома, в течение которых кластер остается уязвим к новым отказам других компонентов. Таким образом, синхронизация реплик томов большого объема может продолжаться несколько часов. Это время на восстановление нужно учитывать при планировании учений с преднамеренным выключением рабочих узлов.

Полный выход из строя компонентов кластера при сохранении доступности Ядра KUMA

В этом случае кластер позволяет какое-то время (до отказа следующего компонента) продолжить работу с Ядром KUMA, выбрать подходящее технологическое окно для восстановления и создать актуальную резервную копию Ядра KUMA.

Чтобы восстановить кластер:

1. Подготовьте новые виртуальные машины или серверы на замену вышедшим из строя компонентам кластера в соответствии с требованиями к установке KUMA.

   На этом этапе можно использовать снимки виртуальных машин, сделанные до установки KUMA.

2. Актуализируйте файл инвентаря k0s.inventory.yml. Если количество сервисов велико и нужно сократить время установки, в секциях файла инвентаря `kuma_collector`, `kuma_correlator` можно оставить по одному хосту, а в секции `kuma_storage` оставить один кластер хранения. Если из строя вышел хост, указанный в секции `kuma_control_plane_master`, то в файле инвентаря k0s.inventory.yml нужно поменять его местами с другим контроллером кластера, указанным в секции `kuma_control_plane`.

3. Установите актуальную версию KUMA с использованием скрипта install.sh и подготовленного файла инвентаря k0s.inventory.yml:

   ```
   sudo ./install.sh k0s.inventory.yml
   ```

4. Убедитесь, что все компоненты кластера работают штатно и отказоустойчивость восстановлена:

   a. Все сервисы k0s запущены:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

   b. Информация о подах и всех рабочих узлах доступна:

   - Чтобы просмотреть состояние тома, выполните следующую команду:

     ```
     sudo k0s kubectl get volume -n longhorn-system -o json | jq
     '.items[0].status.robustness'
     ```

     Статус должен быть `healthy`. Если статус `degraded`, то одна из реплик недоступна или находится в процессе восстановления.

   - Чтобы отслеживать процесс восстановления тома, выполните следующую команду:

     ```
     sudo k0s kubectl get engine -n longhorn-system -o json | jq
     '.items[0].status.rebuildStatus'
     ```

     При корректной работе восстановление не выполняется и команда не вернет никаких значений. Если команда вернет статус `rebuilding`, это означает, что некоторые реплики находятся в процессе восстановления. Мы рекомендуем не вносить изменения в кластер до завершения восстановления.

Восстановление кластера выполнено.

Полный выход из строя компонентов кластера при недоступности Ядра KUMA

> Обязательно наличие резервной копии Ядра KUMA.

Для восстановления кластера требуется предварительно удалить используемый кластер.

Чтобы восстановить кластер:

1. Подготовьте новые виртуальные машины или серверы на замену вышедшим из строя компонентам кластера в соответствии с требованиями к установке KUMA.

   На этом этапе можно использовать снимки виртуальных машин, сделанные до установки KUMA.

2. Подготовьте отдельный файл инвентаря k0s.inventory.yml, предназначенный для удаления кластера. В этом файле инвентаря удалите все хосты, указанные в секциях `kuma_collector`, `kuma_correlator` и `kuma_storage`, чтобы избежать удаления сервисов и необходимости их повторной установки.

3. Удалите неработающий кластер:

   a. Запустите установщик uninstall.sh с подготовленным на шаге 2 файлом инвентаря k0s.inventory.yml:

   ```
   sudo ./uninstall.sh k0s.inventory.yml
   ```

   b. Перезагрузите все хосты из секций файла инвентаря `kuma_worker*` и `kuma_control_plane*`.

   c. После загрузки хостов из секций файла инвентаря `kuma_worker*` и `kuma_control_plane*` снова запустите uninstall.sh c6666 файлом инвентаря k0s.inventory.yml:

   ```
   sudo ./uninstall.sh k0s.inventory.yml
   ```

4. Подготовьте файл инвентаря KUMA для восстановления кластера. За основу следует взять актуальный файл инвентаря установки. Если число внешних сервисов велико и нужно сократить время установки, то в секциях файла инвентаря `kuma_collector`, `kuma_correlator` можно оставить по одному хосту, а в секции `kuma_storage` оставить один кластер хранения. Если время установки сокращать не требуется и перезапуск внешних сервисов KUMA допустим, то файл инвентаря можно использовать без изменений.

5. Установите актуальную версию KUMA с использованием скрипта install.sh и подготовленного файла инвентаря k0s.inventory.yml для восстановления кластера.

6. Восстановите Ядро KUMA из резервной копии.

7. Убедитесь, что Ядро KUMA и остальные сервисы KUMA работают штатно. Для этого перейдите в раздел **Ресурсы** → **Активные сервисы**. Все сервисы должны быть в зеленом статусе.

8. Убедитесь, что все компоненты кластера работают штатно и отказоустойчивость восстановлена:

   a. Все сервисы k0s запущены:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

   b. Информация о подах и всех рабочих узлах доступна:

   - Чтобы просмотреть состояние тома, выполните следующую команду:

     ```
     sudo k0s kubectl get volume -n longhorn-system -o json | jq
     '.items[0].status.robustness'
     ```

     Статус должен быть `healthy`. Если статус `degraded`, то одна из реплик недоступна или находится в процессе восстановления.

   - Чтобы отслеживать процесс восстановления тома, выполните следующую команду:

     ```
     sudo k0s kubectl get engine -n longhorn-system -o json | jq
     '.items[0].status.rebuildStatus'
     ```

     При корректной работе восстановление не выполняется и команда не вернет никаких значений. Если команда вернет статус `rebuilding`, это означает, что некоторые реплики находятся в процессе восстановления. Мы рекомендуем не вносить изменения в кластер до завершения восстановления.

Восстановление кластера выполнено.

Выход из строя балансировщика трафика

Если из строя выходит балансировщик трафика, Ядро KUMA становится недоступно. При этом для восстановления работы балансировщика не требуется удалять или изменять имеющийся кластер или сервисы KUMA. При наличии снимка виртуальной машины балансировщика, сделанного после установки KUMA, вы можете использовать этот снимок. Если снимок виртуальной машины отсутствует или вы хотите использовать новый сервер взамен вышедшего из строя, для восстановления работы кластера потребуется установить балансировщик и настроить его по ранее сохраненной конфигурации.

После восстановления работы балансировщика трафика доступ к кластеру и Ядру KUMA возобновится.

Распределенная установка с Ядром KUMA в кластере Raft

Распределенная установка KUMA с несколькими сервисами Ядра KUMA в кластере позволяет обеспечить отказоустойчивость. Один из сервисов становится лидером; выборы лидера выполняются на основе алгоритма Raft. Операции записи выполняются лидером и транслируются на все серверы кластера. Операции чтения выполняются каждым сервисом из локальной базы SQLite. Таким образом создание нескольких сервисов Ядра KUMA обеспечивает не только отказоустойчивость, но и горизонтальное масштабирование. Допустимо развертывать только нечетное количество сервисов Ядра KUMA.

При необходимости вы можете выполнить следующие действия:

- **Выполнить распределенную установку с Ядром KUMA в кластере Raft с помощью установщика install.sh и файла инвентаря distributed.inventory.yml**.

  В файле инвентаря distributed.inventory.yml необходимо вручную добавить группу kuma_core_peers и указать в этой группе четное количество серверов, где вы планируете установить дополнительные сервисы Ядра KUMA. Также в группе kuma_core вы можете указать параметр raft_node_addr в формате `<FQDN сервера из группы kuma_core, на котором установлено Ядро KUMA>:<порт>`. Этот FQDN будет использоваться для прослушивания сигналов от других узлов.

  После запуска установщика install.sh с подготовленным файлом инвентаря distributed.inventory.yml никакие дополнительные сервисы Ядра KUMA не устанавливаются на серверах автоматически. Установщик только готовит указанные в файле инвентаря серверы к установке сервисов. После завершения работы установщика автоматически установлен только один сервис Ядра KUMA на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

- **Расширить кластер и добавить необходимое количество сервисов Ядра KUMA с помощью установщика expand.sh и файла инвентаря expand.inventory.yml**.

  В файле инвентаря expand.inventory.yml необходимо вручную добавить группу kuma_core_peers и указать в этой группе четное количество серверов, где вы планируете установить дополнительные сервисы Ядра KUMA.

  После запуска установщика expand.sh с подготовленным файлом инвентаря expand.inventory.yml никакие дополнительные сервисы Ядра KUMA не устанавливаются на серверах автоматически. Установщик только готовит указанные в файле инвентаря серверы к установке сервисов. После завершения работы установщика автоматически установлен только один сервис Ядра KUMA на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

- **Обновить распределенную установку KUMA 3.4 до распределенной установки с Ядром KUMA в кластере Raft с помощью установщика install.sh и файла инвентаря distributed.inventory.yml**.

  В файле инвентаря distributed.inventory.yml необходимо вручную добавить группу kuma_core_peers и указать в этой группе четное количество серверов, где вы планируете установить дополнительные сервисы Ядра KUMA. Также в группе kuma_core вы можете указать параметр raft_node_addr в формате `<FQDN сервера из группы kuma_core, на котором установлено Ядро KUMA>:<порт>`. Этот FQDN будет использоваться для прослушивания сигналов от других узлов.

  После запуска установщика с подготовленным файлом инвентаря никакие дополнительные сервисы Ядра KUMA не устанавливаются на серверах автоматически. Установщик только готовит указанные в файле инвентаря серверы к установке сервисов. После завершения работы установщика автоматически установлен только один сервис Ядра KUMA на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

После установки все сервисы Ядра KUMA автоматически добавляются в кластер Raft.

Журналы Ядра KUMA хранятся в директории /opt/kaspersky/kuma/core/`<идентификатор сервиса Ядра KUMA>`/log/core.

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке решения.

2. Сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин, выполнив следующую команду:

   ```
   sudo ssh-keygen -f /root/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   Если на контрольной машине заблокирован доступ root по SSH, сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин с помощью **пользователя из группы sudo**:

   Если у пользователя нет прав sudo, добавьте пользователя в группу sudo:

   ```
   usermod -aG sudo user
   ```

   ```
   ssh-keygen -f /home/< имя пользователя из группы sudo >/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   В результате ключ будет сгенерирован и сохранен в домашней директории пользователя. Вам следует указать полный путь к ключу в файле инвентаря в значении параметра ansible_ssh_private_key_file, чтобы ключ был доступен при установке.

3. Убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

   ```
   sudo ssh-copy-id -i /root/.ssh/id_rsa root@< имя хоста целевой машины >
   ```

   Если на контрольной машине заблокирован доступ root по SSH и вы хотите использовать ключ SSH из домашней директории пользователя из группы sudo, убедитесь, что контрольная машина имеет сетевой доступ ко всем целевым машинам по имени хоста и скопируйте SSH-ключ на каждую целевую машину, выполнив следующую команду:

   ```
   ssh-copy-id -i /home/< имя пользователя из группы sudo >/.ssh/id_rsa < имя пользователя из группы sudo >@< имя хоста целевой машины >
   ```

4. Скопируйте архив с установщиком `kuma-ansible-installer-<номер версии>.tar.gz` на контрольную машину и распакуйте его с помощью следующей команды:

   ```
   sudo tar -xpf kuma-ansible-installer-<номер версии>.tar.gz
   ```

Контрольная машина готова для установки KUMA.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов KUMA:

1. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке.

2. Установите имя хоста. Мы рекомендуем указывать FQDN. Например: kuma1.example.com.

   Имя хоста может начинаться с цифры, но работы Ядра KUMA в кластере Raft нужно использовать имя хоста, которое не начинается с цифры. Если имя хоста начинается с цифры, переименовывать сервер необязательно, достаточно настроить дополнительное имя (FQDN), начинающееся с буквы.

   Не следует изменять имя хоста, используемое KUMA после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами решения.

3. Зарегистрируйте целевую машину в DNS-зоне вашей организации для преобразования имен хостов в IP-адреса.

   Если в вашей организации не используется DNS-сервер, вы можете использовать для преобразования имен файл /etc/hosts. Содержимое файлов можно автоматически создать для каждой целевой машины при установке KUMA.

4. Чтобы получить имя хоста, которое потребуется указать при установке KUMA, выполните следующую команду и запишите результат:

   ```
   hostname -f
   ```

   Целевая машина должна быть доступна по этому имени для контрольной машины.

Целевая машина готова для установки компонентов KUMA.

Подготовка файла инвентаря distributed.inventory.yml для установки KUMA с несколькими сервисами Ядра KUMA в кластере Raft

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible® и созданного пользователем *файла инвентаря* в формате YML с перечнем хостов компонентов KUMA и других параметров.

Чтобы создать файл инвентаря distributed.inventory.yml для установки KUMA с несколькими сервисами Ядра KUMA в кластере Raft:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

2. Скопируйте шаблон distributed.inventory.yml.template и создайте файл инвентаря с именем distributed.inventory.yml:

   ```
   cp distributed.inventory.yml.template distributed.inventory.yml
   ```

3. Отредактируйте параметры файла инвентаря distributed.inventory.yml.

Вручную добавьте в файл инвентаря группу kuma-core-peers и укажите серверы для установки дополнительных сервисов Ядра KUMA. В совокупности общее количество серверов в группах kuma-core и kuma-core-peers должно быть нечетным.

На сервере из группы kuma_core устанавливается сервис kuma-core-00000000-0000-0000-0000-000000000000 (в веб-интерфейсе отображается как core-1). На всех серверах из группы kuma_core_peers последовательно устанавливаются и запускаются сервисы kuma-core-UID (в веб-интерфейсе отображаются как core-<FQDN>), подключаемые к сервису core-1. На каждом сервере может быть установлен только один сервис Ядра KUMA.

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Пример файла инвентаря distributed.inventory.yml для установки KUMA с несколькими сервисами Ядра KUMA в кластере Raft

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
          raft_node_addr: ""
    kuma_core_peers:
      hosts:
        kuma-core-2.example.com:
          ip: 0.0.0.0
        kuma-core-3.example.com:
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
```

```
    kuma-storage-cluster1-server3.example.com:
      ip: 0.0.0.0
      shard: 2
      replica: 1
      keeper: 0
    kuma-storage-cluster1-server4.example.com:
      ip: 0.0.0.0
      shard: 2
      replica: 2
      keeper: 0
    kuma-storage-cluster1-server5.example.com:
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 1
    kuma-storage-cluster1-server6.example.com:
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 2
    kuma-storage-cluster1-server7.example.com:
      ip: 0.0.0.0
      shard: 0
      replica: 0
      keeper: 3
```

Установка в отказоустойчивой конфигурации в кластере Raft

Эта инструкция является частью сценария развертывания и первоначальной настройки.

Установка производится с контрольной машины, при этом все компоненты решения устанавливаются на целевых машинах.

> Перед началом установки убедитесь, что вы выполнили действия по подготовке к установке. Также убедитесь, что у вас есть действующий лицензионный ключ для активации решения.

Чтобы установить Kaspersky SIEM в распределенной конфигурации с Ядром KUMA в кластере Raft, перейдите на контрольную машину и выполните следующие действия:

1 Поместите архив с установщиком на контрольную машину

В личном кабинете на портале Kaspersky CompanyAccount скачайте архив с установщиком, а затем скопируйте архив с установщиком `kuma-ansible-installer-<номер версии KUMA>.tar.gz` на контрольную машину и распакуйте его с помощью следующей команды (потребуется около 2 ГБ дискового пространства):

```
tar -xpf kuma-ansible-installer-<номер версии KUMA>.tar.gz
```

2 Войдите в директорию с установщиком и предоставьте пользователю ОС, от имени которого запускается установщик KUMA, доступ к файлам в директории

Для этого последовательно выполните следующие команды:

```
cd kuma-ansible-installer
chown -R <user_name>:<group> kuma-ansible-installer
```

где:

- <user_name> — пользователь ОС, от имени которого запускается установщик KUMA и которому следует выдать права на директорию с установщиком. Также у пользователя должны быть права на запись в директорию, в которую этот архив будет распаковываться.
- <group> — основная группа пользователя.

3 Активируйте решение

В зависимости от способа активации, выполните следующие действия:

- Файл ключа.

  Поместите файл ключа `license.key` в директорию `<директория установщика>/roles/kuma/files/`:

  ```
  cp <файл ключа>.key <директория установщика>/roles/kuma/files/license.key
  ```

- Код активации.

  Действия не требуются, переходите к следующему пункту инструкции.

  > Активация приложения с помощью кода активации доступна только для KUMA 3.4 и более поздних версий. Для более ранних версий KUMA используется активация приложения файлом ключа.

4 Подготовьте файл инвентаря

1. Скопируйте шаблон `distributed.inventory.yml.template` и создайте файл инвентаря с именем `distributed.inventory.yml`:

   ```
   cp distributed.inventory.yml.template distributed.inventory.yml
   ```

   Шаблон содержит базовый набор параметров, но его недопустимо использовать при установке без изменений.

2. Измените параметры файла инвентаря `distributed.inventory.yml`:

   a. В шаблоне файла инвентаря `distributed.inventory.yml` приведены примеры имен хостов для разных групп сервисов KUMA. Перед установкой замените эти примеры на действительные FQDN в формате `<имя хоста>.<домен>` и при необходимости укажите IPv4-адрес или IPv6-адрес серверов вашей инфраструктуры, на которые будут устанавливаться соответствующие сервисы.

   b. Если вы используете нестандартную директорию для хранения SSH-ключей, укажите полный путь к SSH-ключу в параметре `ansible_ssh_private_key_file` в файле инвентаря в секции `kuma: vars:`, чтобы обеспечить доступ установщика к целевым машинам.

   c. Если вы хотите использовать нестандартный порт для подключения по протоколу SSH в ходе установки, выберите один из следующих вариантов:

      - Если порт одинаковый для группы хостов, укажите порт в параметре `ansible_port` в файле инвентаря в секции `vars`.

      - Если для подключения к каждому хосту используется отдельный нестандартный порт, укажите порт в параметре `ansible_port` для каждого хоста в файле инвентаря.

   d. Если вы хотите, чтобы при установке были созданы предустановленные сервисы (коллектор, коррелятор, хранилище), присвойте параметру `deploy_example_services` значение `true`.

      Предустановленные сервисы будут созданы и автоматически запущены на указанных в файле инвентаря хостах. Созданные сервисы будут доступны в веб-интерфейсе Kaspersky SIEM. Дополнительно устанавливать или запускать их не требуется. При необходимости вы можете удалить предустановленные сервисы.

Ниже приведен пример заполнения файла инвентаря `distributed.inventory.yml` с указанием полного пути к SSH-ключу, без развертывания предустановленных сервисов, с указанием общего нестандартного порта для подключения по протоколу SSH для дополнительных хостов с Ядром KUMA, с указанием отдельного нестандартного порта для подключения по протоколу SSH для коллектора и коррелятора и общего нестандартного порта для группы хостов хранилища.

Пример файла инвентаря distributed.inventory.yml для установки в отказоустойчивой конфигурации в кластере Raft

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
          raft_node_addr: ""
          ansible_port: 2222
    kuma_core_peers:
      vars:
        ansible_port: 2222
      hosts:
        kuma-core-2.example.com:
          ip: 0.0.0.0
        kuma-core-3.example.com:
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
```

```
          ansible_port: 2223
          ip: 0.0.0.0
      kuma_collector:
        hosts:
          kuma-collector-1.example.com:
            ansible_port: 2224
            ip: 0.0.0.0
      kuma_correlator:
        hosts:
          kuma-correlator-1.example.com:
            ansible_port: 2225
            ip: 0.0.0.0
      kuma_storage:
        vars:
          ansible_port: 2226
        hosts:
          kuma-storage-cluster1-server1.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server2.example.com:
            ip: 0.0.0.0
            shard: 1
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server3.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 1
            keeper: 0
          kuma-storage-cluster1-server4.example.com:
            ip: 0.0.0.0
            shard: 2
            replica: 2
            keeper: 0
          kuma-storage-cluster1-server5.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 1
          kuma-storage-cluster1-server6.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 2
          kuma-storage-cluster1-server7.example.com:
            ip: 0.0.0.0
            shard: 0
            replica: 0
            keeper: 3
```

Мы рекомендуем сохранить файл инвентаря, который вы использовали для установки решения. С его помощью вы можете дополнить решение компонентами, обновить или удалить Kaspersky SIEM.

5 Запустите установщик

Запустите установщик `install.sh` с подготовленным файлом инвентаря `distributed.inventory.yml`:

Для пользователя с root-правами

```
./install.sh distributed.inventory.yml
```

Для пользователя без root-прав требуется ввести пароль для повышения привилегий

```
./install.sh distributed.inventory.yml --ask-become-pass
```

6 Ознакомьтесь с условиями Лицензионного соглашения

Если вы не примете условия Лицензионного соглашения, решение не будет установлено.

Если вы хотите принять условия Лицензионного соглашения, при отображении запроса в командной строке введите:

```
yes
```

7 Завершение установки

На этом этапе выполните следующие шаги:

1. Для завершения установки выполните действия в зависимости от способа активации решения:

   Файл ключа

   Если вы активируете решение с помощью файла ключа и поместили файл ключа в директорию `<директория установщика>/roles/kuma/files/`, в результате запуска установщика с файлом инвентаря `distributed.inventory.yml` будут установлены Ядро KUMA на сервере, указанном в секции `kuma_core`, дополнительные Ядра KUMA на серверах, указанных в секции `kuma_core_peers`, и сервис Метрики на сервере, указанном в секции `kuma_metrics`. На указанных в файле инвентаря хостах будут размещены файлы, необходимые для дальнейшей установки и запуска сервисов KUMA, а также будут доступны преднастроенные ресурсы (нормализаторы, правила корреляции, активные листы и другие), отмеченные префиксом **[OOTB]**.

   Сведения о ходе установки, успешно выполненных операциях и возникших ошибках выводятся только в журналы Ядра KUMA, которые хранятся в директории `/opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log/core`.

   После завершения работы установщика войдите в веб-интерфейс.

   Код активации

   Если вы активируете решение с помощью кода активации, будут установлены только Ядро KUMA на сервере, указанном в секции `kuma_core`, дополнительные Ядра KUMA на серверах, указанных в секции `kuma_core_peers`, и сервис Метрики.

   Чтобы завершить установку:

   1. Войдите в веб-интерфейс и укажите код активации.

   2. Запустите установщик `postinstall.sh` с файлом инвентаря `distributed.inventory.yml`:

      ```
      ./postinstall.sh distributed.inventory.yml
      ```

      На хостах, указанных в файле инвентаря, будут размещены файлы, необходимые для дальнейшей установки и запуска сервисов KUMA. В репозитории будут доступны для импорта преднастроенные ресурсы ресурсы (нормализаторы, правила корреляции, активные листы и другие), отмеченные префиксом **[OOTB]**.

Сведения о ходе установки, успешно выполненных операциях и возникших ошибках выводятся только в журналы Ядра KUMA, которые хранятся в директории `/opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log/core`.

2. Определите, будете ли вы использовать балансировщик для кластера Raft и при необходимости настройте балансировщик:

   - Если балансировщик не используется, при установке каждого сервиса нужно будет указывать URL узлов Ядра KUMA через запятую. Вы сможете подключаться к серверам Ядра KUMA напрямую. При переходе между узлами потребуется повторная аутентификация. После успешного входа на новом узле сессия на предыдущем узле будет завершена.

   - Использование балансировщика позволяет распределять нагрузку между узлами кластера и обеспечивает единую точку входа в веб-интерфейс (Single Sign-On, SSO) через AD FS без повторной аутентификации при переключении между узлами кластера, а также возможность доступа к Kaspersky SIEM, если один или несколько хостов с сервисом Ядра KUMA недоступны или вышли из строя.

     Мы рекомендуем использовать один из следующих балансировщиков:

     HAProxy Community Edition

     В этой статье приведен пример настройки HAProxy Community Edition. При необходимости вы можете изменить параметры с учетом ваших потребностей. Конфигурация протестирована с версией пакета 2.4.24-0ubuntu0.22.04.2.

     Чтобы настроить HAProxy Community Edition:

     1. На хосте, где вы устанавливаете балансировщик, запустите консоль командной строки и установите пакет haproxy:

        ```
        sudo apt update && sudo apt install haproxy -y
        ```

     2. Перейдите в директорию /etc/haproxy и измените конфигурационный файл haproxy.cfg, как указано в примере. Порядок секций и параметров в конфигурационном файле должен соответствовать примеру.

        Пример указания параметров в файле haproxy.cfg без использования TLS-сертификата

        ```
        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
        defaults
                log     global
                mode    tcp
                option  tcplog
                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
frontend deploy-raft
    mode tcp
    bind *:7220
    default_backend be_d1
backend be_d1
    mode tcp
    balance roundrobin
    server machine2 kuma-inst-02.avp.ru:7220 check
    server machine3 kuma-inst-03.avp.ru:7220 check
    server machine4 kuma-inst-04.avp.ru:7220 check
```

Пример указания параметров в файле haproxy.cfg с использованием TLS-сертификата

```
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
# Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private
        ssl-default-bind-ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-
GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-
AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
        ssl-default-bind-ciphersuites
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
        ssl-default-bind-options ssl-min-ver TLSv1.3 no-tls-tickets
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
frontend http_front
   bind 0.0.0.0:443 ssl crt kuma-inst-01.avp.ru
   default_backend be_d1 #название группы серверов приложений по умолчанию
backend be_d1 #be_d1 - название группы серверов приложений, используется при
адресации секцией frontend
   balance roundrobin #запросы распределяются поровну между доступными серверами
приложений
   cookie SERVER insert indirect nocache #параметр insert при запросе создает
файл cookie, indirect удаляет файл cookie при каждом входящем запросе перед
пересылкой серверу приложения, #nocache гарантирует отсутствие кеширования между
клиентом и балансировщиком
   option httpchk #запуск HTTP-проверки
   http-check connect port 7220 #для HTTP-проверки используется порт 7220
```

```
   http-check send meth GET #при выполнении проверки используется HTTP-метод GET
   http-check expect status 200 #успешная HTTP-проверка получает от сервера
приложения статус 200 OK
   server machine2 kuma-inst-02.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify
none #параметр inter задает промежуток http-проверки равныйчетырем секундам, для
исключения машины
   server machine3 kuma-inst-03.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify
none #из ротации 2 последовательные проверки должны завершиться ошибкой - fall 2,
для возвращения - 4 должны
   server machine4 kuma-inst-04.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify
none #завершиться успешно - rise 4. Подлинность серверного tls-сертификата не
проверяется - ssl  #verify none
```

3. Сохраните конфигурационный файл haproxy.cfg.

4. Проверьте корректность оформления конфигурационного файла haproxy.cfg с помощью следующей команды:

   ```
   haproxy -f /etc/haproxy/haproxy.cfg -c
   ```

   Если команда проверки вернула ошибку, проверьте, что содержимое конфигурационного файла haproxy.cfg соответствует примеру и при необходимости внесите изменения. Если команда проверки не вернула ошибок, переходите к запуску балансировщика.

5. Запустите балансировщик:

   ```
   sudo systemctl start haproxy
   ```

   Если сервис haproxy требует включения перед запуском, последовательно выполните следующие команды:

   ```
   sudo systemctl enable haproxy
   sudo systemctl start haproxy
   ```

Настройка балансировщика выполнена.

NGINX Open Source

В этой статье приведен пример настройки NGINX Open Source. При необходимости вы можете изменить параметры с учетом ваших потребностей. Конфигурация протестирована с версией пакета 1.18.0-6ubuntu14.6.

Чтобы настроить NGINX Open Source:

1. На хосте, где вы устанавливаете балансировщик, запустите консоль командной строки и установите пакет nginx-common:

   ```
   sudo apt update && sudo apt install nginx-common -y
   ```

2. Перейдите в директорию /etc/nginx и измените конфигурационный файл nginx.conf, как показано в примере. Порядок секций и параметров в конфигурационном файле должен соответствовать примеру.

   Пример указания параметров в файле nginx.conf без использования TLS-сертификата

   ```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;
   error_log /var/log/nginx/error.log;
   include /etc/nginx/modules-enabled/*.conf;
   events {
           worker_connections 768;
   ```

```
}
http {
        sendfile on;
        tcp_nopush on;
        types_hash_max_size 2048;
        server_tokens off;
        server_name_in_redirect off;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        access_log /var/log/nginx/access.log;
        gzip on;
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
}
stream {
    include /etc/nginx/stream-conf.d/*.conf;
        upstream backend {
            server kuma-inst-02.avp.ru:7220;
            server kuma-inst-03.avp.ru:7220;
            server kuma-inst-04.avp.ru:7220;
        }
        server {
            listen 7220;
            proxy_pass backend;
        }
}
```

Пример указания параметров в файле nginx.conf с использованием TLS-сертификата

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
        worker_connections 768;
}
http {
        ##
        # Basic Settings
        ##
        sendfile on;
        tcp_nopush on;
        types_hash_max_size 2048;
        server_tokens off;
        server_name_in_redirect off;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        ##
        # Logging Settings
        ##
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
        ##
        # Gzip Settings
        ##
        gzip on; #
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
    server {
```

```
        listen              443 ssl;
        server_name         kuma-inst-01.avp.ru;
        ssl_certificate     kuma-inst-01.avp.ru;
        ssl_certificate_key kuma-inst-01.avp.ru.key;
        ssl_protocols       TLSv1.3;
        ssl_ciphers         HIGH:!aNULL:!MD5;
        location / { #путь, при обращении по которому происходит передача
запросов группе серверов из proxy_pass
            proxy_pass https://Kuma-UI; #proxy_pass - директива передачи запросов
группе серверов Kuma-UI
        }
    }
    ##
    #max_fails - количество неудачных попыток проверки доступности сервера
решения в пределах интервала.
    #fail_timeout - определяет время, по истечении которого машина будет
исключена из балансировки.
    ##

    upstream Kuma-UI {
        hash $request_uri consistent;
        server kuma-inst-02.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-03.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-04.avp.ru:7220 max_fails=1 fail_timeout=30s;
    }
}
```

3. Сохраните конфигурационный файл nginx.conf.

4. Проверьте корректность оформления конфигурационного файла nginx.cfg с помощью следующей команды:

   ```
   sudo nginx -f /etc/nginx/nginx.conf -t
   ```

   Если команда проверки вернула ошибку, проверьте, что содержимое конфигурационного файла nginx.conf соответствует примеру и при необходимости внесите изменения. Если команда проверки не вернула ошибок, переходите к запуску балансировщика.

5. Запустите балансировщик:

   ```
   sudo systemctl start nginx
   ```

   Если сервис nginx требует включения перед запуском, последовательно выполните следующие команды:

   ```
   sudo systemctl enable nginx
   sudo systemctl start nginx
   ```

Настройка балансировщика выполнена.

3. Если вы настроили использование балансировщика, при необходимости включите доменную аутентификацию через AD FS:

   a. В параметрах настройки AD FS укажите FQDN балансировщика.

   b. В Kaspersky SIEM настройте доменную аутентификацию через AD FS, указав в параметрах FQDN балансировщика.

4. Установите одинаковый часовой пояс на всех серверах, на которых развернуты сервисы Ядра KUMA. После завершения установки часовой пояс при необходимости можно изменить, при этом изменения должны быть одновременно применены на всех узлах кластера Raft.

На этом установка считается завершенной. Вы можете вернуться к сценарию развертывания и продолжить работу с этапа Действия после установки.

Настройка балансировщика для кластера Raft

Использование балансировщика в кластере Raft позволяет распределять нагрузку между узлами кластера и обеспечивает единую точку входа в веб-интерфейс KUMA, а также обеспечивает возможность доступа к KUMA, если один или несколько хостов с сервисом Ядра KUMA недоступны или вышли из строя.

Мы рекомендуем использовать один из следующих балансировщиков:

- HAProxy Community Edition
- NGINX Open Source

Вы можете использовать доменную аутентификацию через AD FS, чтобы на каждом узле кластера Raft не требовалась отдельная аутентификация. Для этого вам необходимо выполнить следующие шаги:

1. В кластере Raft настроить балансировщик.
2. В параметрах настройки AD FS указать FQDN балансировщика.
3. В KUMA настроить доменную аутентификацию через AD FS, указав в параметрах FQDN балансировщика.

Если вы разворачиваете KUMA впервые, после настройки балансировщика вернитесь к свозному сценарию и продолжите работу с этапа Действия после установки.

Пример настройки HAProxy Community Edition

В этой статье приведен пример настройки HAProxy Community Edition. При необходимости вы можете изменить параметры с учетом ваших потребностей. Конфигурация протестирована с версией пакета 2.4.24-0ubuntu0.22.04.2.

Чтобы настроить HAProxy Community Edition:

1. На хосте, где вы устанавливаете балансировщик, запустите консоль командной строки и установите пакет haproxy:

   ```
   sudo apt update && sudo apt install haproxy -y
   ```

2. Перейдите в директорию /etc/haproxy и измените конфигурационный файл haproxy.cfg, как указано в примере. Порядок секций и параметров в конфигурационном файле должен соответствовать примеру.

Пример указания параметров в файле haproxy.cfg без использования TLS-сертификата

```
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
defaults
        log     global
        mode    tcp
        option  tcplog
        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
frontend deploy-raft
    mode tcp
    bind *:7220
    default_backend be_d1
backend be_d1
    mode tcp
    balance roundrobin
    server machine2 kuma-inst-02.avp.ru:7220 check
    server machine3 kuma-inst-03.avp.ru:7220 check
    server machine4 kuma-inst-04.avp.ru:7220 check
```

Пример указания параметров в файле haproxy.cfg с использованием TLS-сертификата

```
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
# Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private
        ssl-default-bind-ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384
        ssl-default-bind-ciphersuites
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
        ssl-default-bind-options ssl-min-ver TLSv1.3 no-tls-tickets
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
frontend http_front
   bind 0.0.0.0:443 ssl crt kuma-inst-01.avp.ru
   default_backend be_d1 #название группы серверов приложений по умолчанию
backend be_d1 #be_d1 - название группы серверов приложений, используется при адресации
секцией frontend
   balance roundrobin #запросы распределяются поровну между доступными серверами
приложений
   cookie SERVER insert indirect nocache #параметр insert при запросе создает файл
cookie, indirect удаляет файл cookie при каждом входящем запросе перед пересылкой
серверу приложения, #nocache гарантирует отсутствие кеширования между клиентом и
балансировщиком
   option httpchk #запуск HTTP-проверки
   http-check connect port 7220 #для HTTP-проверки используется порт 7220
   http-check send meth GET #при выполнении проверки используется HTTP-метод GET
   http-check expect status 200 #успешная HTTP-проверка получает от сервера приложения
статус 200 OK
   server machine2 kuma-inst-02.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none
#параметр inter задает промежуток http-проверки равныйчетырем секундам, для исключения
машины
   server machine3 kuma-inst-03.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none #из
ротации 2 последовательные проверки должны завершиться ошибкой - fall 2, для
возвращения - 4 должны
   server machine4 kuma-inst-04.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none
#завершиться успешно - rise 4. Подлинность серверного tls-сертификата не проверяется -
ssl  #verify none
```

3. Сохраните конфигурационный файл haproxy.cfg.

4. Проверьте корректность оформления конфигурационного файла haproxy.cfg с помощью следующей команды:

   ```
   haproxy -f /etc/haproxy/haproxy.cfg -c
   ```

   Если команда проверки вернула ошибку, проверьте, что содержимое конфигурационного файла haproxy.cfg соответствует примеру и при необходимости внесите изменения. Если команда проверки не вернула ошибок, переходите к запуску балансировщика.

5. Запустите балансировщик:

   ```
   sudo systemctl start haproxy
   ```

   Если сервис haproxy требует включения перед запуском, последовательно выполните следующие команды:

   ```
   sudo systemctl enable haproxy
   sudo systemctl start haproxy
   ```

Настройка балансировщика выполнена.

Пример настройки NGINX Open Source

В этой статье приведен пример настройки NGINX Open Source. При необходимости вы можете изменить параметры с учетом ваших потребностей. Конфигурация протестирована с версией пакета 1.18.0-6ubuntu14.6.

Чтобы настроить NGINX Open Source:

1. На хосте, где вы устанавливаете балансировщик, запустите консоль командной строки и установите пакет nginx-common:

   ```
   sudo apt update && sudo apt install nginx-common -y
   ```

2. Перейдите в директорию /etc/nginx и измените конфигурационный файл nginx.conf, как показано в примере. Порядок секций и параметров в конфигурационном файле должен соответствовать примеру.

   Пример указания параметров в файле nginx.conf без использования TLS-сертификата

   ```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;
   error_log /var/log/nginx/error.log;
   include /etc/nginx/modules-enabled/*.conf;
   events {
           worker_connections 768;
   }
   http {
           sendfile on;
           tcp_nopush on;
           types_hash_max_size 2048;
           server_tokens off;
           server_name_in_redirect off;
           include /etc/nginx/mime.types;
           default_type application/octet-stream;
           access_log /var/log/nginx/access.log;
           gzip on;
           include /etc/nginx/conf.d/*.conf;
           include /etc/nginx/sites-enabled/*;
   }
   stream {
       include /etc/nginx/stream-conf.d/*.conf;
           upstream backend {
               server kuma-inst-02.avp.ru:7220;
               server kuma-inst-03.avp.ru:7220;
               server kuma-inst-04.avp.ru:7220;
           }
           server {
               listen 7220;
               proxy_pass backend;
           }
   }
   ```

   Пример указания параметров в файле nginx.conf с использованием TLS-сертификата

   ```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;
   include /etc/nginx/modules-enabled/*.conf;
   events {
   ```

```
        worker_connections 768;
}
http {
        ##
        # Basic Settings
        ##
        sendfile on;
        tcp_nopush on;
        types_hash_max_size 2048;
        server_tokens off;
        server_name_in_redirect off;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        ##
        # Logging Settings
        ##
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
        ##
        # Gzip Settings
        ##
        gzip on; #
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
    server {
        listen              443 ssl;
        server_name         kuma-inst-01.avp.ru;
        ssl_certificate     kuma-inst-01.avp.ru;
        ssl_certificate_key kuma-inst-01.avp.ru.key;
        ssl_protocols       TLSv1.3;
        ssl_ciphers         HIGH:!aNULL:!MD5;
        location / { #путь, при обращении по которому происходит передача запросов
группе серверов из proxy_pass
            proxy_pass https://Kuma-UI; #proxy_pass - директива передачи запросов
группе серверов Kuma-UI
        }
    }
    ##
    #max_fails - количество неудачных попыток проверки доступности сервера решения в
пределах интервала.
    #fail_timeout - определяет время, по истечении которого машина будет исключена из
балансировки.
    ##

    upstream Kuma-UI {
        hash $request_uri consistent;
        server kuma-inst-02.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-03.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-04.avp.ru:7220 max_fails=1 fail_timeout=30s;
    }
}
```

3. Сохраните конфигурационный файл nginx.conf.

4. Проверьте корректность оформления конфигурационного файла nginx.cfg с помощью следующей команды:

```
sudo nginx -f /etc/nginx/nginx.conf -t
```

Если команда проверки вернула ошибку, проверьте, что содержимое конфигурационного файла nginx.conf соответствует примеру и при необходимости внесите изменения. Если команда проверки не вернула ошибок, переходите к запуску балансировщика.

5. Запустите балансировщик:

   ```
   sudo systemctl start nginx
   ```

   Если сервис nginx требует включения перед запуском, последовательно выполните следующие команды:

   ```
   sudo systemctl enable nginx
   sudo systemctl start nginx
   ```

Настройка балансировщика выполнена.

Расширение кластера Raft

Расширение кластера Raft в KUMA состоит из следующих этапов:

1. Подготовка серверов к установке сервисов Ядра KUMA.

   Установщик expand.sh, который вы запускаете на контрольной машине, готовит на целевых машинах необходимые файлы для последующей установки дополнительных сервисов Ядра KUMA.

2. Создание и установка дополнительных сервисов Ядра KUMA.

   Вам нужно будет создать дополнительные сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA на серверах, указанных в группе kuma_core_peers в файле инвентаря expand.inventory.yml.

3. Обновление файла инвентаря distributed.inventory.yml.

   Перед обновлением KUMA убедитесь, что данные в файле инвентаря `distributed.inventory.yml` соответствуют текущей конфигурации системы.

Подготовка серверов к установке сервисов Ядра KUMA

Чтобы подготовить серверы к последующей установке дополнительных сервисов Ядра KUMA:

1. Убедитесь, что для установки дополнительных сервисов Ядра KUMA вы используете установщик той же версии, который был использован для установки вашего текущего экземпляра KUMA. Полный номер версии должен быть идентичным.

2. На контрольной машине войдите в папку с распакованным установщиком.

   ```
   cd kuma-ansible-installer
   ```

3. В зависимости от типа активации решения, который вы планируете использовать, выберите один из вариантов:

   - Если вы планируете использовать активацию решения файлом ключа, поместите файл ключа в директорию <`папка установщика`>/roles/kuma/files/.

     Файл ключа должен иметь название license.key.

```
sudo cp <файл ключа>.key <папка установщика>/roles/kuma/files/license.key
```

- Если вы планируете использовать активацию решения с помощью лицензионного кода, переходите к следующему пункту инструкции.

4. Скопируйте шаблон expand.inventory.yml.template и создайте файл инвентаря с именем expand.inventory.yml:

   cp expand.inventory.yml.template expand.inventory.yml

   Отредактируйте параметры файла инвентаря expand.inventory.yml и укажите в нем серверы, которые вы хотите добавить, в группе kuma_core_peers. В совокупности общее количество серверов в группах kuma_core и kuma_core_peers должно быть нечетным.

   Пример файла инвентаря expand.inventory.yml для добавления серверов для дополнительных сервисов Ядра KUMA

```
kuma:
  vars:
    no_firewall_actions: false
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core_peers:
      hosts:
        kuma-core-4.example.com:
          ip: 0.0.0.0
        kuma-core-5.example.com:
          ip: 0.0.0.0
```

5. На контрольной машине с доступом root из папки с распакованным установщиком выполните следующую команду:

   ./expand.sh expand.inventory.yml

6. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, решение не будет установлено.

   В зависимости от типа активации решения результатом запуска установщика будет один из следующих вариантов:

   - Если вы планируете использовать активацию решения файлом ключа и поместили файл ключа в директорию <папка установщика>/roles/kuma/files/, в результате запуска установщика с файлом инвентаря expand.inventory.yml серверы, указанные в файле инвентаря, будут подготовлены к установке дополнительных сервисов Ядра KUMA.

   - Если вы планируете использовать активацию решения с помощью лицензионного кода, или планируете предоставить файл ключа позднее, в результате запуска установщика с файлом инвентаря expand.inventory.yml будет установлено только Ядро KUMA.

В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря expand.inventory.yml, появятся файлы для создания и установки дополнительных сервисов Ядра KUMA.

Создание и установка дополнительных сервисов Ядра KUMA

Поскольку сервисы Ядра KUMA состоят из двух частей, клиентской и серверной, вы будете создавать сервисы в два этапа:

1. Создание клиентской части сервиса Ядра KUMA в веб-интерфейсе.

   a. В разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить** и в раскрывающемся списке выберите **Добавить сервис Ядро**.

   b. В открывшемся окне **Добавить сервис Ядро** укажите имя сервиса в поле **Имя сервиса Ядро** и нажмите **Добавить**. Добавленный сервис появится в списке **Сервисы**.

   c. Установите флажок рядом с добавленным сервисом Ядра KUMA и на панели инструментов нажмите ⋮, в открывшемся меню нажмите **Копировать идентификатор**. Идентификатор сервиса Ядра KUMA понадобится для установки сервиса на сервере.

2. Создание серверной части сервиса Ядра KUMA.

   На целевой машине выполните следующую команду.

   ```
   sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN хоста из секции kuma_core, где запущен первый сервис Ядра KUMA>:7210 --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
   ```

   Повторите создание клиентской и серверной части сервиса Ядра KUMA для каждого хоста из группы kuma_core_peers. На каждом хосте может быть установлен только один сервис Ядра KUMA.

Актуализация файла инвентаря distributed.inventory.yml

Впишите группу kuma_core_peers в файле инвентаря distributed.inventory.yml и укажите серверы для дополнительных сервисов Ядра KUMA, которые вы указывали в файле инвентаря expand.inventroy.yml, чтобы в файле инвентаря distributed.inventory.yml были актуальные сведения на случай обновления KUMA.

Результат

Расширение кластера завершено. Сервисы Ядра KUMA добавлены в кластер Raft и подключены к core-1. При установке остальных сервисов KUMA вы можете указать в команде установки несколько URL через запятую для подключения к сервисам Ядра KUMA в кластере Raft.

Удаление узла кластера Raft

Чтобы удалить узел кластера Raft:

1. В веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы** в контекстном меню сервиса Ядра KUMA выберите **Копировать идентификатор**.

2. В разделе **Активные сервисы** выберите сервис Ядра KUMA, установленный на сервере, который вы планируете удалить из кластера Raft, и нажмите **Удалить**.

3. Перейдите на сервер, где установлен удаляемый сервис Ядра KUMA, и остановите сервис с помощью следующей команды:

   ```
   sudo systemctl stop kuma-core-<core_ID>.service
   ```

   где:

   <core_ID> — идентификатор Ядра KUMA, скопированный в веб-интерфейсе.

4. Удалите рабочую директорию.

   ```
   sudo rmdir <directory_path>
   ```

   где:

   <directory_path> — полный путь к рабочей директории, которую вы хотите удалить.

5. Удалите службу systemd.

Узел удален из кластера Raft.

Восстановление узла кластера Raft

Если один или несколько узлов повреждены, но кластер по-прежнему работоспособен, для восстановления узлов кластера Raft доступна следующая последовательность действий:

1. **Удаление узла из кластера Raft**

   Вам нужно удалить поврежденный узел из кластера Raft, а затем заменить его новым узлом.

2. **Создание узла с сервисом Ядра KUMA и добавление его в кластер с помощью параметра --raft.join**

   Вы можете создать новый узел с помощью установщика expand.sh и файла инвентаря expand.inventory.yml, создать сервис Ядра KUMA в веб-интерфейсе и установить сервис Ядра KUMA на сервере, указанном в группе `kuma_core_peers` в файле инвентаря expand.inventory.yml, с помощью команды установки с использованием параметра `--raft.join`. После выполнения команды установки новый узел будет добавлен в кластер Raft.

В результате новый узел получит полную копию состояния узла-лидера. При этом временные файлы, в том числе артефакты фоновых задач, которые могли находиться на потерянном узле, восстановлены не будут.

Восстановление кластера Raft

Если большинство узлов кластера Raft повреждены и кластер неработоспособен, доступны следующие способы восстановления:

- Восстановление кластера Raft из текущего состояния выбранного узла.
- Восстановление кластера Raft из резервной копии.

В результате вы получите новый кластер с одним узлом, на котором установлен сервис Ядра KUMA. Если вы хотите обеспечить отказоустойчивость, вы можете восстановить сервисы Ядра KUMA на прежних узлах или установить сервисы Ядра KUMA на новых узлах и включить эти узлы в кластер Raft. Сбрасывать сертификаты микросервисов, таких как коллекторы, корреляторы, хранилища и другие, не нужно, однако в случае восстановления из резервной копии может потребоваться изменение значения параметра `--core` в файле systemd, чтобы сервисы обращались к нужному Ядру KUMA, если список узлов кластера после восстановления изменился по сравнению с исходным.

Восстановление кластера Raft из текущего состояния узла

Чтобы восстановить кластер Raft из текущего состояния выбранного узла:

1. Подготовьте кластер к восстановлению:

   a. Выберите узел, который станет начальным узлом нового кластера. На этом узле нужно будет остановить сервис Ядра KUMA, но не удалять рабочую директорию и файл systemd.

   b. На всех узлах кластера остановите сервис Ядра KUMA:

   ```
   sudo systemctl stop kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
   ```

   c. На всех узлах кластера, за исключением начального узла, удалите рабочие директории:

   ```
   sudo rmdir <имя_директории>
   ```

   d. На всех узлах кластера, за исключением начального узла, удалите службы systemd.

   На этом этапе все сервисы Ядра KUMA остановлены и серверы готовы к восстановлению кластера.

2. Восстановите кластер Raft с одним Ядром KUMA:

   a. На начальном узле нового кластера Raft создайте следующий файл:

   ```
   sudo touch /opt/kaspersky/kuma/core/<service_id>/raft/.reset
   ```

   b. На начальном узле кластера Raft в файле systemd удалите параметр `--raft.join` и примените изменения, выполнив следующую команду:

   ```
   sudo systemctl daemon-reload
   ```

   c. На начальном узле кластера Raft запустите Ядро KUMA:

   ```
   sudo systemctl start kuma-core-<идентификатор сервиса Ядра KUMA>.service
   ```

   Кластер Raft восстановлен с одним Ядром KUMA. На остальных узлах сервисы Ядра KUMA остановлены, и узлы исключены из кластера.

3. Если вы хотите обеспечить отказоустойчивость кластера Raft, выполните восстановление на остальных узлах кластера:

   - Если вы планируете использовать новые серверы для сервисов Ядра KUMA, используйте установщик expand.sh и файл инвентаря expand.inventory.yml, чтобы развернуть сервисы Ядра KUMA и включить узлы в кластер Raft.

   - Если вы планируете использовать прежние узлы, переустановите сервисы Ядра KUMA с указанием параметра `--raft.join`, чтобы включить узлы в кластер Raft, с помощью следующей команды:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN начального узла кластера>:7210
     --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
     ```

Кластер восстановлен. Сертификаты сервисов, таких как коллекторы, корреляторы, хранилища и другие, сбрасывать не нужно.

Восстановление кластера Raft из резервной копии

Резервная копия не содержит временные файлы, в том числе артефакты фоновых задач.

Чтобы восстановить кластер Raft из резервной копии:

1. Подготовьте кластер к восстановлению:

   a. На каждом узле кластера остановите сервис Ядра KUMA:

   ```
   sudo systemctl stop kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
   ```

   b. На каждом узле, где установлен сервис Ядра KUMA, удалите рабочую директорию:

   ```
   sudo rmdir <имя_директории>
   ```

   c. На каждом узле, где установлен сервис Ядра KUMA, удалите службу systemd.

   На этом этапе все сервисы Ядра KUMA остановлены и серверы готовы к восстановлению кластера.

2. Восстановите кластер Raft с одним сервисом Ядра KUMA:

   a. Выберите сервер, который станет новым начальным узлом кластера Raft, и разверните новый начальный узел кластера без параметра `--raft.join`:

   ```
   sudo /opt/kaspersky/kuma/kuma core --raft.node.listen 0.0.0.0:7209 --raft.node.addr
   "$(hostname -f):7209" --health 0.0.0.0:7208 --internal 0.0.0.0:7210 --private
   0.0.0.0:7220 --cybertrace 0.0.0.0:7222 --rest 0.0.0.0:7223 --install
   ```

   b. Выполните восстановление из резервной копии с помощью REST API.

   Восстановление кластера Raft из резервной копии выполнено. Восстановлен начальный узел кластера с Ядром KUMA.

3. Если вы хотите обеспечить отказоустойчивость кластера Raft, выполните восстановление на остальных узлах кластера:

   - Если вы планируете использовать новые серверы для сервисов Ядра KUMA, используйте установщик expand.sh и файл инвентаря expand.inventory.yml, чтобы развернуть сервисы Ядра KUMA и включить узлы в кластер Raft.

   - Если вы планируете использовать прежние узлы, переустановите сервисы Ядра KUMA с указанием параметра `--raft.join`, чтобы включить узлы в кластер Raft, с помощью следующей команды:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN начального узла кластера>:7210
     --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
     ```

Кластер восстановлен. Сертификаты сервисов, таких как коллекторы, корреляторы, хранилища и другие, сбрасывать не нужно, однако может потребоваться изменение значения параметра `--core` в файле systemd, чтобы сервисы обращались к нужному Ядру KUMA, если список узлов кластера после восстановления изменился по сравнению с исходным.

Изменение имени хоста Ядра KUMA

Чтобы изменить имя хоста на одном из узлов кластера Raft:

1. Удалите два узла Ядра KUMA, на которых не нужно менять имя хоста, выполнив следующие действия:

   a. В веб-интерфейсе KUMA в разделе **Активные сервисы** выберите сервис Ядра KUMA, установленный на сервере, который вы хотите удалить из кластера Raft, и нажмите **Удалить**.

   b. Перейдите на сервер, где установлен удаляемый сервис Ядра KUMA, и остановите сервис:

   ```
   sudo systemctl stop kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
   ```

   c. Создайте резервную копию рабочей директории.

   d. Удалите рабочую директорию:

   ```
   sudo rm -rf /opt/kaspersky/kuma/core/<идентификатор_Ядра_KUMA>
   ```

   e. Удалите файл сервиса systemd:

   ```
   sudo rm /usr/lib/systemd/system/kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
   ```

   Повторите действия, чтобы удалить второй узел Ядра KUMA.

2. Остановите сервис Ядра KUMA на узле, на котором нужно изменить имя хоста, и выключите его автозапуск, выполнив следующие команды:

   ```
   sudo systemctl stop kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
   sudo systemctl disable --now kuma-core-<идентификатор_Ядра_KUMA>
   ```

3. Измените имя хоста на узле:

   ```
   sudo hostnamectl set-hostname <новое_имя_хоста>
   ```

4. В файле /etc/hosts замените старое имя хоста на новое.

5. Перезагрузите узел:

   ```
   sudo reboot
   ```

6. После перезагрузки подключитесь к узлу под новым именем хоста.

7. Перейдите в директорию systemd с конфигурацией сервиса Ядра KUMA и измените параметры запуска:

   - В параметре `--raft.node.addr` укажите новый FQDN узла.

   - Удалите параметр `--raft.join`, если он указан.

8. Примените новые параметры:

   ```
   sudo systemctl daemon-reload
   ```

9. Создайте файл восстановления:

   ```
   sudo -u kuma touch /opt/kaspersky/kuma/core/<идентификатор_Ядра_KUMA>/raft/.reset
   ```

10. Настройте автозапуск Ядра KUMA:

    ```
    sudo systemctl enable --now kuma-core-<идентификатор_Ядра_KUMA>
    ```

11. Запустите Ядро KUMA:

    ```
    sudo systemctl restart kuma-core-<идентификатор_сервиса_Ядра_KUMA>.service
    ```

12. Добавьте в кластер Raft два узла, которые вы удалили на шаге 1, выполнив следующие действия:

    a. В разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить** и в раскрывающемся списке выберите **Добавить сервис Ядро**.

    b. В открывшемся окне **Добавить сервис Ядро** укажите имя сервиса в поле **Имя сервиса Ядро** и нажмите **Добавить**. Добавленный сервис отобразится в списке **Сервисы**.

    c. Установите флажок рядом с добавленным сервисом Ядра KUMA, в панели инструментов откройте меню ⋮ и выберите **Копировать идентификатор**. Идентификатор сервиса Ядра KUMA понадобится для установки сервиса на сервере.

    d. На целевой машине выполните следующую команду.

    ```
    sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN хоста из секции kuma_core, где запущен первый сервис Ядра KUMA>:7210 --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
    ```

Повторите действия, чтобы добавить другой удаленный узел.

Резервное копирование KUMA

Полная резервная копия позволяет восстановить Ядро KUMA после критических сбоев, ошибок обновления, миграции между экземплярами KUMA или потери данных.

Резервная копия содержит все сущности, необходимые для возврата системы в работоспособное состояние:

- алерты;

- активы и учетные записи;

- ресурсы (коллекторы, нормализаторы, правила, словари и другие объекты конфигурации);
- параметры интеграции с внешними системами.

Для переноса или копирования ресурсов следует использовать функции экспорта и импорта ресурсов. Экспорт ресурсов позволяет восстанавливать отдельные объекты конфигурации без восстановления всей инфраструктуры. Это сокращает время восстановления после ошибочных изменений и снижает риск потери актуальных настроек правил, нормализаторов и словарей.

Для обеспечения актуальности резервных копий мы рекомендуем выполнять следующие условия:

1. Создавать полную резервную копию Ядра KUMA с периодичностью не реже одного раза в 7 суток.
2. Экспортировать ресурсы каждые 24 часа.
3. Хранить нескольких поколений резервных копий и контролировать успешность их создания.

Доступны следующие возможности создания резервной копии и восстановления из резервной копии:

- Резервное копирование и восстановление с помощью REST API.
- Резервное копирование и восстановление через веб-интерфейс.

Вы также можете создавать резервные копии отдельных партиций.

Особенности резервного копирования KUMA

- Восстановление данных из резервной копии поддерживается только при сохранении версии KUMA.

  Если в KUMA 4.0 и выше выполнить резервное копирование, а затем восстановить резервную копию на другом устройстве с KUMA 4.0 с помощью REST API (`system/backup → system/restore`), события алертов не восстановятся. В ClickHouse для восстановления событий алертов нужно установить хранилище с тем же идентификатором кластера хранения, где в таблице *kuma.alert_events_local* записи событий будут сопоставлены по ID с алертами. Если хранилище меняется, события алертов можно посмотреть при условии создания резервной копии и последующего восстановления базы данных ClickHouse.

- Резервное копирование коллекторов не требуется, за исключением коллекторов с SQL-подключением. При восстановлении таких коллекторов следует вернуть к начальному значение идентификатора.

Создание резервной копии Ядра KUMA

Доступно создание резервной копии Ядра KUMA одним из следующих способов:

- С помощью REST API.
- Через веб-интерфейс KUMA.

Создание резервной копии Ядра KUMA через веб-интерфейс

Чтобы создать резервную копию Ядра KUMA через веб-интерфейс:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** установите флажок рядом с сервисом Ядра KUMA в зеленом статусе.

2. В меню (⋮) выберите **Резервное копирование** и нажмите **Создать резервную копию**.

   Опция **Создать резервную копию** доступна, если выбран один сервис Ядра KUMA в зеленом статусе.

   Опция недоступна при следующих условиях:

   - Если на предыдущем шаге вы установили флажок рядом с несколькими сервисами.
   - Если сервис Ядра KUMA находится в красном статусе.
   - Если не установлен ни один флажок.
   - Если вы установили флажок рядом с другим типом сервиса.

   Создание резервной копии начнется автоматически. Файл с резервной копией сохраняется в **Загрузки** или папку, которую вы настроили в браузере для скачивания файлов.

   Имя файла резервной копии содержит название сервиса. Если вы создаете резервную копию одного и того же сервиса несколько раз, к имени сервиса добавляется номер копии в скобках. Например, если файл был сохранен впервые, название файла: core-1. При повторном создании резервной копии файл будет называться core-1 (1). Если в настройках вашего браузера включена функция показа уведомления при завершении загрузки, об успешном скачивании файла резервной копии или об ошибке вы сможете узнать из уведомления.

   Метрики не входят в резервную копию.

Создание резервной копии Ядра KUMA выполнено.

Восстановление Ядра KUMA для установки на одном сервере

Восстановить Ядро KUMA из резервной копии можно только в рамках одной версии KUMA. Если вы создадите резервную копию в одной версии KUMA, а восстановление из резервной копии будете выполнять в другой версии, вернется ошибка конфликта версий.

Восстановление Ядра KUMA без смены хоста для core-1

В этой статье описана процедура восстановления Ядра KUMA на том же хосте, где Ядро KUMA было установлено.

Чтобы восстановить Ядро KUMA из резервной копии, воспользуйтесь одним из следующих способов:

- С помощью REST API:

```
curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'
--data-binary '@/backup/backup.tar.gz'
```

- Через веб-интерфейс:

  1. В веб-интерфейсе откройте раздел **Ресурсы** → **Активные сервисы** и установите флажок рядом с сервисом Ядра KUMA в зеленом статусе.

  2. В меню (⋮) выберите **Резервное копирование** → **Восстановить**.

  3. В открывшемся окне выберите файл резервной копии, которую нужно восстановить.

  Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение **Восстановление Ядра KUMA выполнено**.

Ядро KUMA будет восстановлено из резервной копии, и откроется страница входа в веб-интерфейс.

Восстановление Ядра KUMA со сменой хоста для core-1

В этой статье описано восстановление Ядра KUMA из резервной копии на новом хосте.

Чтобы восстановить Ядро KUMA из резервной копии:

1. Установите KUMA на одном сервере на новом хосте с помощью установщика `install.sh` и файла инвентаря `single.inventory.yml`, указав значение параметра:

   ```
   deploy_example_services: false
   ```

   Пример файла инвентаря single.inventory.yml

   ```
   all:
     vars:
       deploy_to_k8s: false
       need_transfer: false
       generate_etc_hosts: false
       deploy_example_services: true
       no_firewall_actions: false
   kuma:
     vars:
       ansible_connection: ssh
       ansible_ssh_private_key_file: <полный путь к файлу с ключом SSH>
       ansible_user: <пользователь из группы sudo>
       ansible_become: true
       ansible_port: 2222
     children:
       kuma_core:
         hosts:
           kuma1.example.com:
       kuma_collector:
         hosts:
           kuma1.example.com
       kuma_correlator:
         hosts:
           kuma1.example.com
       kuma_storage:
   ```

```
      hosts:
        kuma1.example.com:
          shard: 1
          replica: 1
          keeper: 1
    kuma_metrics:
      hosts:
        kuma1.example.com
```

Будет установлено только Ядро KUMA.

2. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью REST API:

     ```
     curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-binary '@/backup/backup.tar.gz'
     ```

   - Через веб-интерфейс:

     a. В веб-интерфейсе откройте раздел **Ресурсы** → **Активные сервисы** и в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

     b. В открывшемся окне выберите файл резервной копии, которую нужно восстановить.

     Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение **Восстановление Ядра KUMA выполнено**.

3. Перевыпустите сертификаты сервисов. Для этого сбросьте сертификаты всех сервисов, кроме Ядра KUMA:

   a. В разделе **Ресурсы** → **Активные сервисы** установите флажок **Выбрать все** и снимите флажок с сервиса Ядра KUMA.

   b. В панели инструментов или в меню (⋮) выберите **Сбросить сертификат**.

   Сертификаты будут сброшены и автоматически перевыпущены для всех сервисов, кроме Ядра KUMA. Перевыпуск сертификатов для Ядра KUMA не требуется, поскольку после восстановления из резервной копии Ядро KUMA уже содержит необходимые данные, включая информацию о сертификатах и доверенных сервисах, которые были восстановлены вместе с резервной копией.

4. На хосте, на котором установлен сервис Метрики, удалите директорию /opt/kaspersky/kuma/metrics/00000000-0000-0000-0000-000000000000/certificates. Это необходимо, чтобы при следующем запуске сервис Метрики не использовал локальные данные прежнего сертификата. Перезапускать сервис Метрики отдельно не требуется. На следующем шаге скрипт change_url.sh переподключит сервис Метрики с новому Ядру KUMA и перезапустит сервис Метрики.

5. Переподключите все сервисы к новому Ядру KUMA и перезагрузите все сервисы одним из следующих способов:

   - Автоматически с помощью скрипта `change_url.sh`, который входит в поставку.

Скрипт массово переподключает сервисы, установленные на хостах, указанных в файле `distributed.inventory.yml`, и перезапускает их. Скрипт обрабатывает сервисы, которые находятся в рабочем состоянии (имеют зеленый статус) на момент выполнения скрипта.

a. Обновите файл инвентаря `distributed.inventory.yml`, указав в секции `kuma_core` FQDN хоста, на который вы перенесли Ядро KUMA и запустите скрипт `change_url.sh` с помощью следующей команды:

```
./change_url.sh distributed.inventory.yml
```

Скрипт переподключит все сервисы, установленные на хостах, указанных в файле инвентаря `distributed.inventory.yml`, к новому Ядру KUMA, а также выполнит перезагрузку всех сервисов.

Сервисы, которые находились в нерабочем состоянии (имели красный статус) во время выполнения скрипта, не будут переподключены автоматически, даже если после этого их статус изменится на зеленый. Для таких сервисов используйте переподключение вручную.

- Вручную с помощью команды. Используйте этот способ, если необходимо переподключить отдельный сервис, например сервис, который не был переподключен скриптом.

```
sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter/metrics --core https://<FQDN>:<port>
--id <service_ID> --api.port <API_port> --install
```

где:

- <FQDN> — полное доменное имя сервера Ядра KUMA.
- <port> — номер порта Ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210).
- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса KUMA.
- <API_port> — порт, используемый для связи с устанавливаемым компонентом.

Ядро KUMA будет восстановлено из резервной копии, и откроется страница входа в веб-интерфейс.

Восстановление Ядра KUMA для распределенной установки

Восстановить Ядро KUMA из резервной копии можно только в рамках одной версии KUMA. Если вы создадите резервную копию в одной версии KUMA, а восстановление из резервной копии будете выполнять в другой версии, вернется ошибка конфликта версий.

Восстановления Ядра KUMA для распределенной установки без смены хоста для core-1

Чтобы восстановить Ядро KUMA из резервной копии, воспользуйтесь одним из следующих способов:

- С помощью REST API:

```
curl -k --request POST '<FQDN>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-
binary '@/backup/backup.tar.gz'
```

где:

- <FQDN> — полное доменное имя сервера Ядра KUMA.
- <token> — токен для API-запросов.

- Через веб-интерфейс:

  a. В веб-интерфейсе откройте раздел **Ресурсы** → **Активные сервисы** и в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

  b. В открывшемся окне выберите файл резервной копии, которую нужно восстановить.

  Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение **Восстановление Ядра KUMA выполнено**.

Ядро KUMA будет восстановлено из резервной копии, и откроется страница входа в веб-интерфейс.

После завершения восстановления Ядро KUMA продолжит работу с существующими сервисами. Дополнительная настройка сервисов не требуется.

Восстановление Ядра KUMA со сменой хоста для core-1

В этой инструкции описано восстановление Ядра KUMA из резервной копии на новом хосте. Остальные сервисы KUMA остаются на прежних хостах.

После восстановления необходимо перевыпустить сертификаты сервисов и переподключить их к Ядру KUMA на новом хосте.

Чтобы восстановить Ядро KUMA из резервной копии:

1. Подготовьте новый экземпляр KUMA, выполнив установку KUMA на одном сервере на новом хосте с помощью установщика `install.sh` и файла инвентаря `single.inventory.yml`, указав значение параметра:

   ```
   deploy_example_services: false
   ```

   На указанном в файле инвентаря хосте будет установлено только Ядро KUMA.

   Новый экземпляр Ядра KUMA не содержит данных прежней инфраструктуры. В этом экземпляре будет восстановлена резервная копия.

2. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью REST API:

     ```
     curl -k --request POST '<FQDN>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --
     data-binary '@/backup/backup.tar.gz'
     ```

где:

- <FQDN> — полное доменное имя сервера Ядра KUMA.
- <token> — токен для API-запросов.

- Через веб-интерфейс:

  a. В веб-интерфейсе откройте раздел **Ресурсы** → **Активные сервисы** и в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

  b. В открывшемся окне выберите файл резервной копии, которую нужно восстановить.

  После завершения восстановления откроется страница входа в веб-интерфейс KUMA.

  Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение **Восстановление Ядра KUMA выполнено**.

После восстановления Ядра KUMA из резервной копии выполните следующие действия, чтобы сервисы могли подключиться к Ядру KUMA на новом хосте.

3. Перевыпустите сертификаты сервисов. Для этого сбросьте сертификаты всех сервисов, кроме Ядра KUMA:

   a. В разделе **Ресурсы** → **Активные сервисы** установите флажок **Выбрать все** и снимите флажок с сервиса Ядра KUMA.

   b. В панели инструментов или в меню (⋮) выберите **Сбросить сертификат**.

   Сертификаты будут сброшены и автоматически перевыпущены для всех сервисов, кроме Ядра KUMA. Перевыпуск сертификатов для Ядра KUMA не требуется, поскольку после восстановления из резервной копии Ядро KUMA уже содержит необходимые данные, включая информацию о сертификатах и доверенных сервисах, которые были восстановлены вместе с резервной копией.

4. На хосте, на котором установлен сервис Метрики, удалите директорию /opt/kaspersky/kuma/metrics/00000000-0000-0000-0000-000000000000/certificates. Это необходимо, чтобы при следующем запуске сервис Метрики не использовал локальные данные прежнего сертификата. Перезапускать сервис Метрики отдельно не требуется. На следующем шаге скрипт change_url.sh переподключит сервис Метрики с новому Ядру KUMA и перезапустит сервис Метрики.

5. Переподключите все сервисы к новому Ядру KUMA и перезагрузите все сервисы одним из следующих способов:

   - Автоматически с помощью скрипта `change_url.sh`, который входит в поставку.

Скрипт массово переподключает сервисы, установленные на хостах, указанных в файле `distributed.inventory.yml`, и перезапускает их. Скрипт обрабатывает сервисы, которые находятся в рабочем состоянии (имеют зеленый статус) на момент выполнения скрипта.

a. Обновите файл инвентаря `distributed.inventory.yml`, указав в секции `kuma_core` FQDN хоста, на который вы перенесли Ядро KUMA и запустите скрипт `change_url.sh` с помощью следующей команды:

```
./change_url.sh distributed.inventory.yml
```

Скрипт переподключит все сервисы, установленные на хостах, указанных в файле инвентаря `distributed.inventory.yml`, к новому Ядру KUMA, а также выполнит перезагрузку всех сервисов.

Сервисы, которые находились в нерабочем состоянии (имели красный статус) во время выполнения скрипта, не будут переподключены автоматически, даже если после этого их статус изменится на зеленый. Для таких сервисов используйте переподключение вручную.

- Вручную с помощью команды. Используйте этот способ, если необходимо переподключить отдельный сервис, например сервис, который не был переподключен скриптом.

```
sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter/metrics --core https://<FQDN>:<port>
--id <service_ID> --api.port <API_port> --install
```

где:

- <FQDN> — полное доменное имя сервера Ядра KUMA.
- <port> — номер порта Ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210).
- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса KUMA.
- <API_port> — порт, используемый для связи с устанавливаемым компонентом.

После выполнения процедуры все сервисы KUMA будут подключены к восстановленному Ядру KUMA на новом хосте.

Восстановление Ядра KUMA в кластере Kubernetes

Временная недоступность отдельных компонентов кластера

Если отдельные компоненты кластера временно недоступны, например, из-за временного отключения питания сервера, сетевой недоступности или сбоя, потребовавшего перезагрузки сервера или виртуальной машины, для восстановления не требуется пересоздание виртуальных машин или замены серверов. Доступность Ядра KUMA в этом случае определяется набором оставшихся в работе компонентов. В этот же сценарий входят сбои на сервере или виртуальной машине, которые не требуют переустановки операционной системы и которые можно оперативно устранить заменой отдельных частей или изменением конфигурации ПО.

После восстановления работы и доступности всех компонентов работоспособность кластера восстанавливается автоматически, но некоторое время выполняются переходные операции, такие как синхронизация реплик тома, в течение которых кластер остается уязвим к новым отказам других компонентов. Таким образом, синхронизация реплик томов большого объема может продолжаться несколько часов. Это время на восстановление нужно учитывать при планировании учений с преднамеренным выключением рабочих узлов.

Полный выход из строя компонентов кластера при сохранении доступности Ядра KUMA

В этом случае кластер позволяет какое-то время (до отказа следующего компонента) продолжить работу с Ядром KUMA, выбрать подходящее технологическое окно для восстановления и создать актуальную резервную копию Ядра KUMA.

Чтобы восстановить кластер:

1. Подготовьте новые виртуальные машины или серверы на замену вышедшим из строя компонентам кластера в соответствии с требованиями к установке KUMA.

   На этом этапе можно использовать снимки виртуальных машин, сделанные до установки KUMA.

2. Актуализируйте файл инвентаря k0s.inventory.yml. Если количество сервисов велико и нужно сократить время установки, в секциях файла инвентаря `kuma_collector`, `kuma_correlator` можно оставить по одному хосту, а в секции `kuma_storage` оставить один кластер хранения. Если из строя вышел хост, указанный в секции `kuma_control_plane_master`, то в файле инвентаря k0s.inventory.yml нужно поменять его местами с другим контроллером кластера, указанным в секции `kuma_control_plane`.

3. Установите актуальную версию KUMA с использованием скрипта install.sh и подготовленного файла инвентаря k0s.inventory.yml:

   ```
   ./install.sh k0s.inventory.yml
   ```

   У пользователя, из-под которого будет запускаться установка решения, должны быть права на архив с установщиком, а также права на запись в директорию, в которую этот архив будет распаковываться.

4. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью REST API.

   - Через веб-интерфейс:

     a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

     b. В появившемся окне с файловой системой выберите файл резервной копии, который следует использовать для восстановления.

     Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение "Восстановление Ядра KUMA выполнено".

     После восстановления будет выполнен переход на страницу входа в веб-интерфейс KUMA.

5. Убедитесь, что все компоненты кластера работают штатно и отказоустойчивость восстановлена:

   a. Все сервисы k0s запущены:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

b. Информация о подах и всех рабочих узлах доступна:

- Чтобы просмотреть состояние тома, выполните следующую команду:

  ```
  sudo k0s kubectl get volume -n longhorn-system -o json | jq
  '.items[0].status.robustness'
  ```

  Статус должен быть `healthy`. Если статус `degraded`, то одна из реплик недоступна или находится в процессе восстановления.

- Чтобы отслеживать процесс восстановления тома, выполните следующую команду:

  ```
  sudo k0s kubectl get engine -n longhorn-system -o json | jq
  '.items[0].status.rebuildStatus'
  ```

  При корректной работе восстановление не выполняется и команда не вернет никаких значений. Если команда вернет статус `rebuilding`, это означает, что некоторые реплики находятся в процессе восстановления. Мы рекомендуем не вносить изменения в кластер до завершения восстановления.

6. Установите сервис Метрики с помощью установщика expand.sh и файла инвентаря expand.inventory.yml. Перенесите данные из директории metrics на хост с восстановленным Ядром KUMA.

Восстановление кластера выполнено.

Полный выход из строя компонентов кластера при недоступности Ядра KUMA

> Обязательно наличие резервной копии Ядра KUMA.

Для восстановления кластера требуется предварительно удалить используемый кластер.

Чтобы восстановить кластер:

1. Подготовьте новые виртуальные машины или серверы на замену вышедшим из строя компонентам кластера в соответствии с требованиями к установке KUMA.

   На этом этапе можно использовать снимки виртуальных машин, сделанные до установки KUMA.

2. Подготовьте отдельный файл инвентаря k0s.inventory.yml, предназначенный для удаления кластера. В этом файле инвентаря удалите все хосты, указанные в секциях `kuma_collector`, `kuma_correlator` и `kuma_storage`, чтобы избежать удаления сервисов и необходимости их повторной установки.

3. Удалите неработающий кластер:

   a. Запустите установщик uninstall.sh с подготовленным на шаге 2 файлом инвентаря k0s.inventory.yml:

   ```
   ./uninstall.sh k0s.inventory.yml
   ```

   b. Перезагрузите все хосты из секций файла инвентаря `kuma_worker*` и `kuma_control_plane*`.

   c. После загрузки хостов из секций файла инвентаря `kuma_worker*` и `kuma_control_plane*` снова запустите uninstall.sh c6666 файлом инвентаря k0s.inventory.yml:

   ```
   ./uninstall.sh k0s.inventory.yml
   ```

4. Подготовьте файл инвентаря KUMA для восстановления кластера. За основу следует взять актуальный файл инвентаря установки. Если число внешних сервисов велико и нужно сократить время установки, то в секциях файла инвентаря `kuma_collector`, `kuma_correlator` можно оставить по одному хосту, а в секции `kuma_storage` оставить один кластер хранения. Если время установки сокращать не требуется и перезапуск внешних сервисов KUMA допустим, то файл инвентаря можно использовать без изменений.

5. Установите актуальную версию KUMA с использованием скрипта install.sh и подготовленного файла инвентаря k0s.inventory.yml для восстановления кластера.

6. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью REST API.

   - Через веб-интерфейс:

     a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

     b. В появившемся окне с файловой системой выберите файл резервной копии, который следует использовать для восстановления.

     Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение "Восстановление Ядра KUMA выполнено".

     После восстановления будет выполнен переход на страницу входа в веб-интерфейс KUMA.

7. Убедитесь, что Ядро KUMA и остальные сервисы KUMA работают штатно. Для этого перейдите в раздел **Ресурсы** → **Активные сервисы**. Все сервисы должны быть в зеленом статусе.

8. Убедитесь, что все компоненты кластера работают штатно и отказоустойчивость восстановлена:

   a. Все сервисы k0s запущены:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

   b. Информация о подах и всех рабочих узлах доступна:

   - Чтобы просмотреть состояние тома, выполните следующую команду:

     ```
     sudo k0s kubectl get volume -n longhorn-system -o json | jq
     '.items[0].status.robustness'
     ```

     Статус должен быть `healthy`. Если статус `degraded`, то одна из реплик недоступна или находится в процессе восстановления.

   - Чтобы отслеживать процесс восстановления тома, выполните следующую команду:

     ```
     sudo k0s kubectl get engine -n longhorn-system -o json | jq
     '.items[0].status.rebuildStatus'
     ```

     При корректной работе восстановление не выполняется и команда не вернет никаких значений. Если команда вернет статус `rebuilding`, это означает, что некоторые реплики находятся в процессе восстановления. Мы рекомендуем не вносить изменения в кластер до завершения восстановления.

9. Установите сервис Метрики с помощью установщика expand.sh и файла инвентаря expand.inventory.yml. Перенесите данные из директории metrics на хост с восстановленным Ядром KUMA.

Восстановление кластера выполнено.

Восстановление Ядра KUMA в кластере Raft

Восстановления Ядра KUMA в кластере Raft без смены хоста для core-1

В этой инструкции описано восстановление Ядра KUMA из резервной копии на хосте из секции файла инвентаря `kuma_core`, где Ядро KUMA было изначально установлено. В этом сценарии необходимо будет "разобрать" кластер и удалить сервис KUMA из веб-интерфейса, восстановить Ядро KUMA из резервной копии на хосте из секции файла инвентаря `kuma_core`, установить сервис Ядра KUMA на дополнительных узлах и объединить их в кластер, чтобы обеспечить отказоустойчивость, установить сервис Метрики и перенести существующие данные метрик на новый хост.

Восстановить Ядро KUMA из резервной копии можно только в рамках одной версии KUMA. Если вы создадите резервную копию в одной версии KUMA, а восстановление из резервной копии будете выполнять в другой версии, вернется ошибка конфликта версий.

Чтобы восстановить Ядро KUMA из резервной копии:

1. Подготовьте кластер к восстановлению. Для этого на каждом хосте, указанном в секции `kuma_core_peers` в файле инвентаря выполните следующие действия:

   a. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом Ядра KUMA и на панели инструментов или в меню (⋮) выберите **Копировать идентификатор**.

   Идентификатор сервиса Ядра KUMA понадобится вам для остановки сервиса на хосте.

   b. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом Ядра KUMA и на панели инструментов или в меню (⋮) выберите **Удалить**.

   c. На хосте кластера Raft, где установлен сервис Ядра KUMA, в консоли командной строки остановите сервис Ядра KUMA:

   `sudo systemctl stop kuma-core-<идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе>.service`

   d. На хосте кластера Raft, где установлен сервис Ядра KUMA, удалите рабочую директорию:

   `sudo rmdir <имя_директории>`

   e. На хосте кластера Raft, где установлен сервис Ядра KUMA, удалите службу systemd.

   На этом этапе все серверы готовы к восстановлению кластера.

2. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью метода REST API post/system/restore.

   - Через веб-интерфейс:

     a. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

     b. В появившемся окне с файловой системой выберите файл резервной копии, который следует использовать для восстановления.

     Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение "Восстановление Ядра KUMA выполнено".

     После восстановления Ядра KUMA будет выполнен переход на страницу входа в веб-интерфейс.

3. Если вы хотите обеспечить отказоустойчивость кластера Raft, выполните восстановление на остальных узлах кластера:

   - Если вы планируете использовать новые серверы для сервисов Ядра KUMA, используйте установщик expand.sh и файл инвентаря expand.inventory.yml, чтобы развернуть сервисы Ядра KUMA и включить узлы в кластер Raft.

   - Если вы планируете использовать прежние узлы, переустановите сервисы Ядра KUMA с указанием параметра `--raft.join`, чтобы включить узлы в кластер Raft, с помощью следующей команды:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN начального узла кластера>:7210
     --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
     ```

4. Установите сервис Метрики с помощью установщика expand.sh и файла инвентаря expand.inventory.yml. Перенесите данные из директории metrics на хост с восстановленным Ядром KUMA.

Восстановление Ядра KUMA из резервной копии выполнено.

Восстановления Ядра KUMA в кластере Raft со сменой хоста для core-1

В этой инструкции описано восстановление Ядра KUMA из резервной копии на новом хосте. В этом сценарии необходимо будет полностью "разобрать" кластер и удалить сервис KUMA из веб-интерфейса, установить с нуля Ядро KUMA на новом хосте, выполнить на этом хосте восстановление Ядра KUMA из резервной копии, установить сервис Ядра KUMA на дополнительных узлах и объединить их в кластер, чтобы обеспечить отказоустойчивость, переподключить сервисы к Ядру KUMA на новом хосте, установить сервис Метрики и перенести существующие данные метрик на новый хост, перенастроить балансировщик.

Восстановить Ядро KUMA из резервной копии можно только в рамках одной версии KUMA. Если вы создадите резервную копию в одной версии KUMA, а восстановление из резервной копии будете выполнять в другой версии, вернется ошибка конфликта версий.

Чтобы восстановить Ядро KUMA из резервной копии:

1. Подготовьте кластер к восстановлению. Для этого на всех хостах кластера Raft выполните следующие действия:

   a. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом Ядра KUMA и на панели инструментов или в меню (⋮) выберите **Копировать идентификатор**.

      Идентификатор сервиса Ядра KUMA понадобится вам для остановки сервиса на хосте.

   b. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом Ядра KUMA и на панели инструментов или в меню (⋮) выберите **Удалить**.

   c. На хосте кластера Raft, где установлен сервис Ядра KUMA, в консоли командной строки остановите сервис Ядра KUMA с помощью следующей команды:

      ```
      sudo systemctl stop kuma-core-<идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе>.service
      ```

   d. На хосте кластера Raft, где установлен сервис Ядра KUMA, удалите рабочую директорию:

      ```
      sudo rmdir <имя_директории>
      ```

   e. На хосте кластера Raft, где установлен сервис Ядра KUMA, удалите службу systemd.

      На этом этапе все сервисы Ядра KUMA остановлены и серверы готовы к восстановлению кластера.

2. Выполните установку KUMA на одном сервере на новом хосте с помощью установщика install.sh и файла инвентаря single.inventory.yml, указав значение параметра `deploy_example_services: false`.

   На указанном в файле инвентаря хосте будет установлено только Ядро KUMA.

3. Восстановите Ядро KUMA из резервной копии одним из следующих способов:

   - С помощью метода REST API post/system/restore.
   - Через веб-интерфейс:

     a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

     b. В появившемся окне с файловой системой выберите файл резервной копии, который следует использовать для восстановления.

        Если в вашем браузере настроены уведомления, в правом верхнем углу отобразится сообщение "Восстановление Ядра KUMA выполнено".

   Восстановлен начальный узел кластера с Ядром KUMA. После восстановления начального узла будет выполнен переход на страницу входа в веб-интерфейс.

4. Если вы хотите обеспечить отказоустойчивость кластера Raft, выполните восстановление на остальных узлах кластера:

   - Если вы планируете использовать новые серверы для сервисов Ядра KUMA, используйте установщик expand.sh и файл инвентаря expand.inventory.yml, чтобы развернуть сервисы Ядра KUMA и включить узлы в кластер Raft.

   - Если вы планируете использовать прежние узлы, переустановите сервисы Ядра KUMA с указанием параметра `--raft.join`, чтобы включить узлы в кластер Raft, с помощью следующей команды:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN начального узла кластера>:7210
     --id <идентификатор сервиса Ядра KUMA, скопированный в веб-интерфейсе> --install
     ```

5. Переподключите сервисы к новому Ядру KUMA с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter --core
   https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних
   коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса,
   скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с
   устанавливаемым компонентом> --install
   ```

6. Установите сервис Метрики с помощью установщика expand.sh и файла инвентаря expand.inventory.yml. Перенесите данные из директории metrics на хост с восстановленным Ядром KUMA.

7. Перенастройте балансировщик, указав хосты с установленным сервисом Ядра KUMA.

Восстановление из резервной копии выполнено.

Изменение конфигурации KUMA

Доступны следующие изменения конфигурации KUMA.

- **Расширение установки "все в одном" до распределенной**.

  В этой статье описано, как расширить конфигурацию развертывания на одном сервере до распределенной, а также приведен пример расширения конфигурации.

  Переход на распределенную схему развертывания может потребоваться, например, в следующих случаях:

  - Необходимость сбалансировать нагрузку при увеличении нагрузки сверх рекомендуемой и снижении производительности.

  - Обеспечение высокой отказоустойчивости любого из компонентов.

  - Требования высокой доступности сервисов хранилища (большое количество сложных поисковых запросов).

  - Особенности ИТ-инфраструктуры, например обособленные сетевые сегменты со слабыми каналами связи.

  - Административные особенности. Например, есть требования разделить доступ между командами – администратор серверов, требования регуляторов – локальное хранение данных.

Чтобы расширить конфигурацию развертывания на одном сервере до распределенной:

1. Создайте резервную копию KUMA.

2. Подготовьте целевые машины для расширения конфигурации развертывания на одном сервере до распределенной.

3. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

```
cd kuma-ansible-installer
```

4. Подготовьте файл инвентаря `expand.inventory.yml`:

   a. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

   b. В файле инвентаря `expand.inventory.yml` в секциях `kuma_<название компонента>` введите FQDN целевых машин для установки сервисов KUMA.

5. На контрольной машине с доступом root из директории с распакованным установщиком выполните следующую команду:

```
./expand.sh expand.inventory.yml
```

   В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для установки сервисов KUMA.

6. Сбросьте сертификаты для сервисов, которые вы планируете перенести на целевые машины, указанные в файле инвентаря `expand.inventory.yml`:

   a. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.

   b. В списке сервисов установите флажки для необходимых сервисов и в контекстном меню выберите **Сбросить сертификат**.

   KUMA автоматически сгенерирует новый сертификат для каждого сервиса, для которого был сброшен сертификат.

7. На целевых машинах, указанных в файле инвентаря `expand.inventory.yml`, установите серверные части сервисов KUMA, серверная и веб-часть которых уже были созданы для конфигурации развертывания на одном сервере: хранилища, коллекторы, корреляторы и другие необходимые.

8. Перезапустите сервисы KUMA, серверные части которых были установлены на предыдущем шаге:

   a. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.

   b. В списке сервисов установите флажки для необходимых сервисов и в контекстном меню выберите **Перезапустить**.

9. В файле инвентаря `distributed.inventory.yml` укажите FQDN добавленных в конфигурацию целевых машин, чтобы в файле были актуальные сведения на случай обновления KUMA.

Пример расширения конфигурации развертывания на одном сервере до распределенной

В организации развернута конфигурация KUMA на одном сервере – `kuma.example.com`. Сотрудники ИБ организации пришли к выводу, что одного сервера недостаточно и необходимо добавить два дополнительных сервера хранения и дополнительный сервер коллекторов: `storage-1.example.com`, `storage-2.example.com` и `remote-collector.example.com`.

Для решения этой задачи необходимо расширить конфигурацию KUMA на одном сервере до распределенной:

1. Создайте резервную копию KUMA.

2. Подготовьте целевые машины `storage-1.example.com`, `storage-2.example.com` и `remote-collector.example.com` для добавления новых серверов хранения и сервера коллекторов в конфигурацию KUMA.

3. Подготовьте файл инвентаря `expand.inventory.yml`:

   a. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

   b. В файле `expand.inventory.yml` `kuma_<название компонента>` введите FQDN целевых машин для установки сервисов хранения, коллекторов и других необходимых серверов.

   Пример содержимого файла expand.inventory.yml для добавления новых серверов хранения и сервера коллекторов

   ```
   all:
     vars:
       deploy_to_k8s: false
       need_transfer: false
       generate_etc_hosts: false
       deploy_example_services: false
       no_firewall_actions: false
   kuma:
     vars:
       ansible_connection: ssh
       ansible_user: root
     children:
       kuma_collector:
         hosts:
   ```

```
        remote-collector.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 0
          keeper: 1
        storage-1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 0
          keeper: 0
        storage-2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
```

4. На контрольной машине `kuma.example.com` с доступом root из директории с распакованным установщиком выполните следующую команду:

   ```
   ./expand.sh expand.inventory.yml
   ```

   В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для создания и установки сервисов KUMA.

5. Сбросьте сертификаты для сервисов хранилища и коллектора, которые вы планируете перенести на целевые машины, указанные в файле инвентаря `expand.inventory.yml`:

   a. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.

   b. В списке сервисов установите флажки для сервисов хранилища и коллектора и в контекстном меню выберите **Сбросить сертификат**.

   KUMA автоматически сгенерирует новые сертификаты для сервисов хранилища и коллектора.

6. На целевых машинах, указанных в файле инвентаря `expand.inventory.yml`, установите серверные части хранилища и коллектора, серверная и веб-часть которых уже были созданы для конфигурации развертывания на одном сервере.

7. Перезапустите сервисы хранилища и коллектора:

   a. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**.

   b. В списке сервисов установите флажки для сервисов хранилища и коллектора и в контекстном меню выберите **Перезапустить**.

8. Если необходимо, создайте точки назначения с актуальными данными о хранилищах и коллекторах.

9. В файле инвентаря `distributed.inventory.yml` укажите FQDN добавленных в конфигурацию целевых машин, чтобы в файле были актуальные сведения на случай обновления KUMA.

Расширение конфигурации развертывания на одном сервере до распределенной завершено.

- **Добавление серверов для коллекторов в распределенную установку**.

В этой статье описано, как добавить один или несколько серверов в существующую инфраструктуру, чтобы затем установить на них коллекторы и таким образом перераспределить нагрузку. Вы можете использовать инструкцию в качестве примера и адаптировать ее под свои потребности.

Чтобы добавить серверы в распределенную установку:

1. Убедитесь, что на целевых машинах соблюдены аппаратные и программные требования, а также требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, М ОС.

2. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

```
cd kuma-ansible-installer
```

3. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Измените параметры файла инвентаря `expand.inventory.yml` и укажите в нем серверы, которые вы хотите добавить, в секции `kuma_collector`.

Пример файла инвентаря expand.inventory.yml для добавления серверов для коллекторов

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
      hosts:
        kuma-additional-collector1.example.com:
          ip: 0.0.0.0
        kuma-additional-collector2.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
    kuma_storage:
      hosts:
```

5. На контрольной машине с доступом root из директории с распакованным установщиком выполните следующую команду:

```
./expand.sh expand.inventory.yml
```

В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для создания и установки коллектора.

6. Создайте и установите коллекторы. Поскольку коллекторы KUMA состоят из клиентской и серверной части, выполните следующие два шага:

   a. Создайте клиентскую часть коллектора, которая включает в себя набор ресурсов и сервис коллектора.

      Чтобы создать набор ресурсов для коллектора, в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор** и настройте параметры. Подробнее см. Создание коллектора.

      На последнем шаге мастера настройки, после того, как вы нажмете **Создать и сохранить**, будет создан набор ресурсов для коллектора и автоматически будет создан сервис коллектора. Также будет автоматически сформирована команда для установки сервиса на сервере. Эта команда отобразится на экране. Скопируйте команду установки и переходите к следующему шагу.

   b. Создайте серверную часть коллектора:

      1. На целевой машине выполните скопированную на предыдущем шаге команду. Команда будет выглядеть подобным образом, но все параметры будут автоматически заполнены:

         ```
         sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --install
         ```

         Сервис коллектора будет установлен на целевой машине. Вы можете проверить статус сервиса в веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы**.

      2. Повторите команду на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`.

7. Укажите добавленные серверы в файле инвентаря `distributed.inventory.yml`, чтобы в нем были актуальные сведения на случай обновления KUMA.

Добавление серверов завершено.

- **Добавление серверов для корреляторов в распределенную установку**.

В этой статье описано, как добавить один или несколько серверов в существующую инфраструктуру, чтобы затем установить на них коррелятор и таким образом перераспределить нагрузку. Вы можете использовать инструкцию в качестве примера и адаптировать ее под свои потребности.

Чтобы добавить серверы в распределенную установку:

1. Убедитесь, что на целевых машинах соблюдены аппаратные и программные требования, а также требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, М ОС.

2. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

3. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

4. Измените параметры файла инвентаря `expand.inventory.yml` и укажите в нем серверы, которые вы хотите добавить, в секции `kuma_correlator`.

   Пример файла инвентаря expand.inventory.yml для добавления серверов для корреляторов

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
      hosts:
        kuma-additional-correlator1.example.com:
          ip: 0.0.0.0
        kuma-additional-correlator2.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
```

5. На контрольной машине с доступом root из директории с распакованным установщиком выполните следующую команду:

```
./expand.sh expand.inventory.yml
```

   В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для создания и установки коррелятора.

6. Создайте и установите корреляторы. Поскольку корреляторы KUMA состоят из клиентской и серверной частей, выполните следующие два шага:

   a. Создайте клиентскую часть коррелятора, которая включает в себя набор ресурсов и сервис коррелятора.

      Чтобы создать набор ресурсов для коррелятора, в веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор** и настройте параметры. Подробнее см. Создание коррелятора.

      На последнем шаге мастера настройки, после того, как вы нажмете **Создать и сохранить**, будет создан набор ресурсов для коррелятора и автоматически будет создан сервис коррелятора. Также будет автоматически сформирована команда для установки сервиса на сервере. Эта команда отобразится на экране. Скопируйте команду установки и переходите к следующему шагу.

   b. Создайте серверную часть коррелятора:

      1. На целевой машине выполните скопированную на предыдущем шаге команду. Команда будет выглядеть подобным образом, но все значения всех параметров будут автоматически присвоены:

```
sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN сервера Ядра KUMA>:<порт, используемый
Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор
сервиса, скопированный из веб-интерфейса KUMA> --install
```

         Сервис коррелятора будет установлен на целевой машине. Вы можете проверить статус сервиса в веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы**.

      2. Повторите команду на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`.

7. Укажите добавленные серверы в файле инвентаря `distributed.inventory.yml`, чтобы в нем были актуальные сведения на случай обновления KUMA.

Добавление серверов завершено.

- **Добавление серверов в существующий кластер хранения**.

В этой статье описывается порядок добавления нескольких серверов в существующий кластер хранения. Вы можете использовать инструкцию в качестве примера и адаптировать ее под свои потребности.

Чтобы добавить серверы в существующий кластер хранения:

1. Убедитесь, что на целевых машинах соблюдены аппаратные и программные требования, а также требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, М ОС.

2. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

```
cd kuma-ansible-installer
```

3. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Измените параметры файла инвентаря `expand.inventory.yml` и укажите в нем серверы, которые вы хотите добавить, в секции `storage`. В приведенном примере в секции `storage` указаны серверы для установки двух шардов, каждый из которых будет содержать по две реплики. В файле инвентаря `expand.inventory.yml` следует указать только FQDN. Роли шардов и реплик вы будете назначать позднее в веб-интерфейсе KUMA, последовательно выполняя шаги инструкции. Вы можете адаптировать приведенный пример файла под свои потребности.

   Пример файла инвентаря expand.inventory.yml для добавления серверов в существующий кластер хранения

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server8.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server9.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server10.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server11.example.com:
 ip: 0.0.0.0
```

5. На контрольной машине с доступом root из директории с распакованным установщиком выполните следующую команду:

```
./expand.sh expand.inventory.yml
```

   В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для создания и установки хранилища.

6. Поскольку вы добавляете серверы в существующий кластер хранения, создавать отдельное хранилище не требуется. Измените параметры хранилища существующего кластера:

   a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Хранилища** выберите существующее хранилище и откройте его для изменения.

   b. В разделе **Узлы кластера ClickHouse** нажмите **Добавить узлы** и в появившихся полях для нового узла укажите роли. В примере показано, как указать идентификаторы, чтобы добавить в существующий кластер два шарда, каждый из которых содержит две реплики. Вы можете адаптировать пример под свои потребности.

   Пример добавления узлов

   ```
   Узлы кластера ClickHouse
   <существующие узлы>
   Полное доменное имя: kuma-storage-cluster1server8.example.com
   Идентификатор шарда: 1
   Идентификатор реплики: 1
   Идентификатор кипера: 0
   Полное доменное имя: kuma-storage-cluster1server9.example.com
   Идентификатор шарда: 1
   Идентификатор реплики: 2
   Идентификатор кипера: 0
   Полное доменное имя: kuma-storage-cluster1server9.example.com
   Идентификатор шарда: 2
   Идентификатор реплики: 1
   Идентификатор кипера: 0
   Полное доменное имя: kuma-storage-cluster1server10.example.com
   Идентификатор шарда: 2
   Идентификатор реплики: 2
   Идентификатор кипера: 0
   ```

   c. Сохраните параметры хранилища.

   Теперь можно создать сервисы хранилища для каждого узла кластера ClickHouse.

7. Создайте сервис хранилища:

   a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

   b. В открывшемся окне **Выберите сервис** выберите измененное на предыдущем шаге хранилище и нажмите **Создать сервис**. Повторите для каждого добавляемого узла хранилища ClickHouse.

   Количество созданных сервисов должно равняться количеству добавляемых узлов в кластере ClickHouse, то есть 4 узла – 4 сервиса. Созданные сервисы хранилища отображаются в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы**.

8. Установите сервисы хранилища на каждом сервере, используя идентификатор сервиса:

   a. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** выберите нужный сервис хранилища и нажмите **Копировать идентификатор**.

   Идентификатор сервиса будет скопирован в буфер обмена и понадобится при выполнении команды установки сервиса.

b. Выполните на целевой машине следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --install
```

Сервис хранилища будет установлен на целевой машине. Вы можете проверить статус сервиса в веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы**.

c. Последовательно выполните команду установки сервиса хранилища на каждой целевой машине, указанной в секции storage в файле инвентаря `expand.inventory.yml`. На каждой машине в команде установки требуется указывать уникальный идентификатор сервиса в рамках кластера.

9. Примените изменения в работающем кластере. Для этого в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** установите флажок рядом со всеми сервисами хранилища в кластере, который вы расширяете, и нажмите **Обновить параметры**. Изменения будут применены без остановки сервисов.

10. Укажите добавленные серверы в файле инвентаря `distributed.inventory.yml`, чтобы в нем были актуальные сведения на случай обновления KUMA.

Добавление серверов в кластер хранения завершено.

- **Добавление дополнительного кластера хранения**.

В этой статье описано, как добавить дополнительный кластер хранения в существующую инфраструктуру. Вы можете использовать инструкцию в качестве примера и адаптировать ее под свои потребности.

Чтобы добавить дополнительный кластер хранения:

1. Убедитесь, что на целевых машинах соблюдены аппаратные и программные требования, а также требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, М ОС.

2. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

```
cd kuma-ansible-installer
```

3. Скопируйте шаблон `expand.inventory.yml.template` и создайте файл инвентаря с именем `expand.inventory.yml`:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Измените параметры файла инвентаря `expand.inventory.yml` и укажите в нем серверы, которые вы хотите добавить, в секции `storage`. В приведенном примере в секции `storage` указаны серверы для установки 3 выделенных киперов и 2 шардов, каждый из которых будет содержать по 2 реплики. В файле инвентаря `expand.inventory.yml` следует указать только FQDN. Роли киперов, шардов и реплик вы будете назначать позднее в веб-интерфейсе KUMA, последовательно выполняя шаги инструкции. Вы можете адаптировать этот пример под свои потребности.

Пример файла инвентаря expand.inventory.yml для добавления дополнительного кластера хранения

```
kuma:
  vars:
    ansible_connection: ssh
```

```
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
    kuma_storage:
      hosts:
        kuma-storage-cluster2-server1.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server2.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server3.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server4.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server5.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server6.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server7.example.com:
          ip: 0.0.0.0
```

5. На контрольной машине с доступом root из директории с распакованным установщиком выполните следующую команду:

```
./expand.sh expand.inventory.yml
```

В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря `expand.inventory.yml`, появятся файлы для создания и установки хранилища.

6. Создайте и установите хранилище. Для каждого кластера хранения следует создавать отдельное хранилище, то есть 3 кластера хранения – 3 хранилища. Поскольку хранилище состоит из клиентской и серверной частей, выполните следующие два шага:

   a. Создайте клиентскую часть хранилища, которая включает в себя набор ресурсов и сервис хранилища:

      1. Чтобы создать набор ресурсов для хранилища, в веб-интерфейсе KUMA в разделе **Ресурсы** → **Хранилища** нажмите **Добавить хранилище** и настройте параметры. В разделе **Узлы кластера ClickHouse** укажите роли для каждого добавляемого сервера: кипер, шард, реплика. Подробнее см. Создание набора ресурсов для хранилища.

         Созданный набор ресурсов для хранилища отображается в разделе **Ресурсы** → **Хранилища**. Теперь можно создать сервисы хранилища для каждого узла кластера ClickHouse.

      2. Чтобы создать сервис хранилища, в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

         В открывшемся окне **Выберите сервис** выберите созданный на шаге a. набор ресурсов для хранилища и нажмите **Создать сервис**. Повторите для каждого узла хранилища ClickHouse.

         Количество созданных сервисов должно равняться количеству узлов в кластере ClickHouse, то есть 50 узлов – 50 сервисов. Созданные сервисы хранилища отображаются в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор сервиса.

   b. На целевой машине создайте серверную часть хранилища:

      1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** выберите нужный сервис хранилища и нажмите **Копировать идентификатор**.

         Идентификатор сервиса будет скопирован в буфер обмена, он понадобится для выполнения команды установки сервиса.

2. Сформируйте и выполните на целевой машине следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --install
```

   Сервис хранилища будет установлен на целевой машине. Вы можете проверить статус сервиса в веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы**.

3. Последовательно выполните команду установки сервиса хранилища на каждой целевой машине, указанной в секции `storage` в файле инвентаря `expand.inventory.yml`. На каждой машине в команде установки требуется указывать уникальный идентификатор сервиса в рамках кластера.

Выделенные киперы запускаются автоматически сразу после установки и отображаются в разделе **Ресурсы** → **Активные сервисы** в зеленом статусе. Сервисы на остальных узлах хранилища могут не запускаться до тех пор, пока не будут установлены сервисы для всех узлов данного кластера. До этого момента сервисы могут отображаться в красном статусе. Это нормальное поведение для создания нового кластера хранения или добавления узлов в существующий кластер хранения. Как только будет выполнена команда установки сервисов на всех узлах кластера, все сервисы переходят в зеленый статус.

7. Укажите добавленные серверы в файле инвентаря `distributed.inventory.yml`, чтобы в нем были актуальные сведения на случай обновления KUMA.

Добавление дополнительного кластера хранения завершено.

- **Удаление серверов из распределенной установки**.

При необходимости вы можете удалить сервер из распределенной установки.

Чтобы удалить сервер из распределенной установки:

1. Удалите все сервисы с сервера, который вы планируете удалить из распределенной установки:

2. Удалите сервер из файла инвентаря `distributed.inventory.yml`, чтобы в файле инвентаря были актуальные сведения на случай обновления KUMA.

Сервер удален из распределенной установки.

- **Удаление кластера хранения из распределенной установки**.

При необходимости вы можете удалить кластер хранения.

Чтобы удалить один или несколько кластеров хранения из распределенной установки:

1. Получите идентификатор сервиса хранилища. Для этого в разделе **Ресурсы** → **Активные сервисы** откройте контекстное меню удаляемого сервиса и нажмите **Копировать идентификатор**.

2. Удалите сервис хранилища на каждом сервере кластера, подлежащем удалению из распределенной установки:

   a. Удалите серверную часть сервиса хранилища, выполнив на целевой машине следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <storage> --id <идентификатор сервиса> --uninstall
```

   Повторите для каждого сервера.

b. Удалите клиентскую часть сервиса в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** → **Удалить**.

Сервис удален.

3. Удалите серверы из секции `storage` в файле инвентаря `distributed.inventory.yml`, чтобы в файле инвентаря были актуальные сведения на случай обновления KUMA или изменения конфигурации.

Кластер удален из распределенной установки.

- **Перенос Ядра KUMA в новый кластер Kubernetes**.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log

    - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
    - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
  - Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
  - На хосте с Ядром переносит директории:
    - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
    - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

  После проверки корректности переноса Ядра в кластер данные директории можно удалить.

  В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

  При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

  Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Обновление предыдущих версий KUMA

Обновление выполняется одинаково на всех хостах с использованием установщика и файла инвентаря.

Схема обновления версий:

2.0.x → 2.1.3 → 3.0.3 → 3.2.x → 3.4.x → 4.0

2.1.x → 2.1.3 → 3.0.3 → 3.2.x → 3.4.x → 4.0

2.1.3 → 3.0.3 → 3.2.x → 3.4.x → 4.0

3.0.x → 3.0.3 → 3.2.x → 3.4.x → 4.0

Если вы вносили изменения в unit-файлы сервисов KUMA в директории /usr/lib/systemd/system вручную, при обновлении с предыдущей версии KUMA эти изменения будут потеряны. При необходимости внесите изменения повторно после обновления решения.

Обновление с версии 2.0.x до 2.1.3

Чтобы установить KUMA версии 2.1.3 поверх версии 2.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить резервную копию для версии 2.0.

   Резервные копии KUMA, созданные в версии 2.0 и ниже, не подлежат восстановлению в версии 2.1.3. Это означает, что невозможно установить KUMA 2.1.3 и восстановить в ней резервную копию KUMA 2.0.

   Сразу после обновления KUMA до версии 2.1.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. Убедитесь в совместимости версий MongoDB, выполнив на устройстве с Ядром KUMA следующую последовательность команд:

   ```
   cd /opt/kaspersky/kuma/mongodb/bin/
   ./mongo
   use kuma
   db.adminCommand({getParameter: 1, featureCompatibilityVersion: 1})
   ```

   Если версия компонента отличается от 4.4, задайте значение 4.4 с помощью следующей команды:

   ```
   db.adminCommand({ setFeatureCompatibilityVersion: "4.4" })
   ```

4. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

5. Если в кластере ClickHouse у вас есть кипер, развернутый на отдельном устройстве, перед обновлением установите сервис хранилища на том же устройстве:

   - Используйте существующее хранилище кластера, чтобы создать в веб-интерфейсе сервис хранилища для кипера.
   - Установите сервис на устройстве с выделенным кипером ClickHouse.

6. В файле инвентаря укажите те же хосты, которые использовались при установке KUMA версии 2.0.X. Присвойте значение `false` следующим параметрам:

   ```
   deploy_to_k8s false
   need_transfer false
   deploy_example_services false
   ```

   При работе установщика по такому файлу инвентаря обновляются все компоненты KUMA до версии 2.1.3. Также производится перенастройка имеющихся сервисов и ресурсов хранилища на хостах из группы kuma_storage:

   - Удаляются systemd-сервисы ClickHouse.
   - Удаляются сертификаты из директории /opt/kaspersky/kuma/clickhouse/certificates.
   - Заполняются поля Идентификатор шарда, Идентификатор реплики, Идентификатор кипера и Переопределение параметров ClickHouse для каждого узла в ресурсе хранилища на основании значений из инвентаря и конфигурационных файлов сервиса на хосте. В дальнейшем управление ролями каждого узла вы будет выполнять в веб-интерфейсе KUMA.

- Удаляются все существующие файлы конфигурации из директории /opt/kaspersky/kuma/clickhouse/cfg (далее они будут генерироваться сервисом хранилища).

- Изменяется значение параметра LimitNOFILE (секция Service) с 64000 на 500000 в systemd-сервисах kuma-storage.

7. Если вы используете правила сегментации алертов, подготовьте данные для переноса существующих правил и сохраните. На следующем этапе вы сможете использовать эти данные, чтобы заново создать правила. При обновлении правила сегментации алертов не переносятся автоматически.

8. Чтобы выполнить обновление, вам понадобится действительный пароль от пользователя admin. Если вы забыли пароль от пользователя admin, обратитесь в Службу технической поддержки, чтобы сбросить действующий пароль и воспользуйтесь новым паролем, чтобы выполнить обновление на следующем этапе.

Обновление KUMA

1. В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

  Процесс обновления полностью повторяет процесс установки.

  Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**.

  Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

  1. Подготовьте файл инвентаря k0s.inventory.yml.

     В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

  2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

1. При обновлении на системах, которые содержат большие данные и при этом работают на предельных ресурсах, после того, как вы введете пароль администратора, система может вернуть сообщение об ошибке Wrong admin password. Если вы указываете верный пароль, KUMA может все равно возвращать ошибку, потому что KUMA не удалось запустить сервис Ядра из-за ошибки по таймауту и предельных ресурсов. Если вы введете пароль администратора трижды, не дожидаясь завершения установки, обновление может завершиться фатальной ошибкой. Устраните ошибку по таймауту, чтобы продолжить обновление.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Создайте заново правила сегментации алертов.
3. Вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Обновление с версии 2.1.x до 2.1.3

Чтобы установить KUMA версии 2.1.3 поверх версии 2.1.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить резервную копию для версии 2.1.x.

   Резервные копии KUMA, созданные в версии ниже 2.1.3, не подлежат восстановлению в версии 2.1.3. Это означает, что невозможно установить KUMA 2.1.3 и восстановить в ней резервную копию KUMA 2.1.x.

   Сразу после обновления KUMA до версии 2.1.3 создайте резервную копию.
2. Убедитесь, что соблюдены все требования к установке решения.
3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.
4. Чтобы выполнить обновление, вам понадобится действительный пароль от пользователя admin. Если вы забыли пароль от пользователя admin, обратитесь в Службу технической поддержки, чтобы сбросить действующий пароль и воспользуйтесь новым паролем, чтобы выполнить обновление на следующем этапе.

Обновление KUMA

1. В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

   - Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.
   - Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

   Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

   Процесс обновления полностью повторяет процесс установки.

Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.

- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

  После проверки корректности переноса Ядра в кластер данные директории можно удалить.

  В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

  При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

  Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

2. При обновлении на системах, которые содержат большие данные и при этом работают на предельных ресурсах, после того, как вы введете пароль администратора, система может вернуть сообщение об ошибке Wrong admin password. Если вы указываете верный пароль, KUMA может все равно возвращать ошибку, потому что KUMA не удалось запустить сервис Ядра из-за ошибки по таймауту и предельных ресурсов. Если вы введете пароль администратора трижды, не дожидаясь завершения установки, обновление может завершиться фатальной ошибкой. Устраните ошибку по таймауту, чтобы продолжить обновление.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Обновление с версии 2.1.3 до 3.0.3

Чтобы установить KUMA версии 3.0.3 поверх версии 2.1.3, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.3.

   Резервные копии KUMA, созданные в версии 2.1.3 и ниже, не подлежат восстановлению в версии 3.0.3. Это означает, что невозможно установить KUMA 3.0.3 и восстановить в ней резервную копию KUMA 2.1.3.

   Сразу после обновления KUMA до версии 3.0.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Известные ограничения

1. Поскольку в 3.0.2 иерархическая структура не поддерживается, при обновлении с версии 2.1.3 до 3.0.2 все хосты с KUMA становятся независимыми.

2. Для действующих пользователей при обновлении с 2.1.3 до 3.0.2 не выполняется обновление универсального макета панели мониторинга.

   Возможное решение: перезапустите сервис Ядра kuma-core.service - данные будут обновляться с заданным для макета интервалом.

Обновление с версии 3.0.x до 3.0.3

Чтобы установить KUMA версии 3.0.3 поверх версии 3.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.x.

   Резервные копии KUMA, созданные в версии ниже 3.0.3, не подлежат восстановлению в версии 3.0.3. Это означает, что невозможно установить KUMA 3.0.3 и восстановить в ней резервную копию KUMA 3.0.x.

   Сразу после обновления KUMA до версии 3.0.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Известные ограничения

Для действующих пользователей при обновлении с 3.0.x до 3.0.3 не выполняется обновление универсального макета панели мониторинга.

Возможное решение: перезапустите сервис Ядра kuma-core.service - данные будут обновляться с заданным для макета интервалом.

Обновление с версии 3.0.3 до 3.2.x

Чтобы установить KUMA версии 3.2.x поверх версии 3.0.3, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.3.

   Резервные копии KUMA, созданные в версии 3.0.3 и ниже, не подлежат восстановлению в версии 3.2.x. Это означает, что невозможно установить KUMA 3.2.x и восстановить в ней резервную копию 3.0.3.

   Сразу после обновления KUMA до версии 3.2.x создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. Убедитесь, что имя хоста Ядра KUMA не начинается с цифры. Обновление до версии 3.2.x не может быть выполнено успешно, если имя хоста Ядра KUMA начинается с цифры. Потребуется ряд мероприятий, чтобы успешно выполнить обновление. Обратитесь в техническую поддержку за дополнительными инструкциями.

4. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**. Для дальнейшего обновления используйте файл инвентаря k0s.inventory.yml с параметром need_transfer: false, поскольку перенос Ядра KUMA в кластер Kubernetes уже выполнен и больше не требуется.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Известные ограничения

1. Для действующих пользователей при обновлении с 3.0.3 до 3.2.x не выполняется обновление универсального макета панели мониторинга.

   Возможное решение: перезапустите сервис Ядра kuma-core.service - данные будут обновляться с заданным для макета интервалом.

2. Если после обновления остался отображается старый сервис Ядра kuma-core.service, после завершения установки выполните следующую команду:

   sudo systemctl reset-failed

   После выполнения команды старый сервис перестанет отображаться, а новый сервис успешно запустится.

Обновление с версии 3.2.0 или 3.2.1 до 3.4

Чтобы установить KUMA версии 3.4 поверх версии 3.2.0 или 3.2.1, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 3.2.

   Резервные копии KUMA, созданные в версии 3.2 и ниже, не подлежат восстановлению в версии 3.4. Это означает, что невозможно установить KUMA 3.4 и восстановить в ней резервную копию 3.2.x.

   Сразу после обновления KUMA до версии 3.4 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. Убедитесь, что имя хоста Ядра KUMA не начинается с цифры. Обновление до версии 3.4 не может быть выполнено успешно, если имя хоста Ядра KUMA начинается с цифры. Если имя хоста Ядра KUMA начинается с цифры, потребуется ряд мероприятий, чтобы успешно выполнить обновление. Обратитесь в техническую поддержку за дополнительными инструкциями.

4. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

5. Проверьте количество и актуальность источников событий, для которых отображается красный статус, в разделе **Состояние источников** → **Список источников событий** и для неактуальных источников событий выполните одно из следующих действий:

   - удалите неактуальные источники событий;
   - измените параметры политик мониторинга, примененных к неактуальным источникам событий, так, чтобы они соответствовали актуальному потоку событий;
   - для политик мониторинга, примененных к неактуальным источникам событий, отключите рассылку уведомлений.

После обновления KUMA для всех источников событий с красным статусом, для которых настроена отправка уведомлений о срабатывании политики, будут отправлены уведомления на указанные адреса электронной почты.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.
- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Если вы хотите выполнить обновление с распределенной установки до распределенной установки в отказоустойчивой конфигурации, выполните обновление распределенной установки, а затем выполните **Перенос Ядра в кластер Kubernetes**. Для дальнейшего обновления используйте файл инвентаря k0s.inventory.yml с параметром need_transfer: false, поскольку перенос Ядра KUMA в кластер Kubernetes уже выполнен и больше не требуется.

Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

1. Подготовьте файл инвентаря k0s.inventory.yml.

   В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin
- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

После проверки корректности переноса Ядра в кластер данные директории можно удалить.

В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты KUMA.

Обновление KUMA успешно выполнено.

Известные ограничения

1. Для действующих пользователей при обновлении с 3.2.0 или 3.2.1 до 3.4 не выполняется обновление универсального макета панели мониторинга.

   Возможное решение: перезапустите сервис Ядра kuma-core.service - данные будут обновляться с заданным для макета интервалом.

2. Если после обновления остался отображается старый сервис Ядра kuma-core.service, после завершения установки выполните следующую команду:

   sudo systemctl reset-failed

   После выполнения команды старый сервис перестанет отображаться, а новый сервис успешно запустится.

Обновление с версии 3.4.x до 4.0

Чтобы установить KUMA версии 4.0 поверх версии 3.4.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 3.4.x.

   Резервные копии KUMA, созданные в версии 3.4.x и ниже, не подлежат восстановлению в версии 4.0. Это означает, что невозможно установить KUMA 4.0 и восстановить в ней резервную копию 3.4.x.

   Сразу после обновления KUMA до версии 4.0 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. Проверьте имя хоста Ядра KUMA.

   Имя хоста может начинаться с цифры, если это соответствует принятой в организации схеме именования. Однако для работы сервисов KUMA с Raft нужно имя хоста, которое не начинается с цифры.

   Если имя хоста начинается с цифры, переименовывать сервер необязательно. Настройте дополнительное имя (FQDN), начинающееся с буквы, выполнив следующие действия:

   a. В файле `/etc/hosts` добавьте запись:

   ```
   <IP_address> <new_fqdn> <fqdn> <hostname>
   ```

   где:

   `<IP_address>` – IP-адрес сервера;

   `<new_fqdn>` – дополнительное имя хоста;

   `<fqdn>` – исходное FQDN;

   `<hostname>` – короткое имя хоста.

   b. На DNS-сервере создайте CNAME-запись, в которой `<new_fqdn>` указывает на `<fqdn>`.

После настройки используйте дополнительное имя для сервисов KUMA с Raft. Исходное имя хоста изменять не нужно.

4. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

5. Проверьте количество и актуальность источников событий, для которых отображается красный статус, в разделе **Состояние источников** → **Список источников событий** и для неактуальных источников событий выполните одно из следующих действий:

   - удалите неактуальные источники событий;
   - измените параметры политик мониторинга, примененных к неактуальным источникам событий, так, чтобы они соответствовали актуальному потоку событий;
   - для политик мониторинга, примененных к неактуальным источникам событий, отключите рассылку уведомлений.

   После обновления KUMA для всех источников событий с красным статусом, для которых настроена отправка уведомлений о срабатывании политики, будут отправлены уведомления на указанные адреса электронной почты.

6. Для установки с Ядром KUMA в кластере Kubernetes запустите скрипт для определения размера данных метрик на томе Ядра KUMA 3.4, при необходимости задайте или переопределите значения параметров `metrics_transfer_job_timeout`, `metrics_disk_request`, `core_disk_request` в файле инвентаря k0s.inventory.yml, а затем перейдите к обновлению.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения.
- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации с Ядром KUMA в кластере Kubernetes .

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Вы можете изменить тип установки следующим образом:

- Если вы хотите выполнить обновление с распределенной установки до установки с Ядром KUMA в кластере Kubernetes, выполните обновление распределенной установки до последней версии, а затем выполните **Перенос Ядра в кластер Kubernetes**. Для дальнейшего обновления используйте файл инвентаря k0s.inventory.yml с параметром `need_transfer: false`, поскольку перенос Ядра KUMA в кластер Kubernetes уже выполнен и больше не требуется.

  Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

  1. Подготовьте файл инвентаря k0s.inventory.yml.

     В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

  2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin

- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

  После проверки корректности переноса Ядра в кластер данные директории можно удалить.

  В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

  При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

  Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

- Если вы хотите обновить KUMA в распределенной установке до последней версии KUMA с Ядром в кластере Raft, в файле инвентаря distributed.inventory.yml необходимо вручную добавить группу `kuma_core_peers` и указать в этой группе четное количество серверов, где вы планируете установить дополнительные сервисы Ядра KUMA. Также в группе `kuma_core` и `kuma_core_peers` вы можете указать параметр `raft_node_addr` в формате `<FQDN сервера из группы kuma_core, на котором установлено Ядро KUMA>:<порт>`, если у сервера есть несколько разных FQDN. Указанный в параметре `raft_node_addr` FQDN будет использоваться для прослушивания сигналов от других узлов.

  После запуска установщика с подготовленным файлом инвентаря никакие дополнительные сервисы Ядра KUMA не устанавливаются на серверах автоматически. Установщик только готовит указанные в файле инвентаря серверы к установке сервисов. После завершения работы установщика автоматически установлен только один сервис Ядра KUMA на сервере указанном в группе `kuma_core`. После завершения работы установщика вам необходимо вручную создать сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA с уникальным идентификатором на каждом сервере, указанном в группе `kuma_core_peers`.

  После обновления все существующие сервисы KUMA будут подключены к Ядру KUMA на сервере из группы `kuma_core`. При дальнейшей установке новых сервисов вы можете указать несколько URL через запятую в команде установки, чтобы подключить сервисы к Ядрам KUMA в кластере Raft.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты KUMA.
3. Выполните миграцию событий алертов из MongoDB в ClickHouse.
4. Укажите хранилище для новых событий алертов в параметрах наполнения алертов.

Обновление KUMA успешно выполнено.

Известные ограничения

1. Для действующих пользователей при обновлении с 3.4.x до 4.0 не выполняется обновление универсального макета панели мониторинга.

   Возможное решение: перезапустите сервис Ядра kuma-core.service - данные будут обновляться с заданным для панели мониторинга интервалом.

2. Если после обновления остался отображается старый сервис Ядра kuma-core.service, после завершения установки выполните следующую команду:

   ```
   sudo systemctl reset-failed
   ```

   После выполнения команды старый сервис перестанет отображаться, а новый сервис успешно запустится.

Обновление с версии 4.0.x до 4.2

Чтобы установить KUMA версии 4.2 поверх версии 4.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA. При необходимости вы сможете восстановить данные из резервной копии для версии 4.0.x.

   Резервные копии KUMA, созданные в версии 4.0.x и ниже, не подлежат восстановлению в версии 4.2. Это означает, что невозможно установить KUMA 4.2 и восстановить в ней резервную копию 4.0.x.

   Сразу после обновления KUMA до версии 4.2 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке решения.

3. Проверьте имя хоста Ядра KUMA.

   Имя хоста может начинаться с цифры, если это соответствует принятой в организации схеме именования. Однако для работы сервисов KUMA с Raft нужно имя хоста, которое не начинается с цифры.

   Если имя хоста начинается с цифры, переименовывать сервер необязательно. Настройте дополнительное имя (FQDN), начинающееся с буквы, выполнив следующие действия:

   a. В файле `/etc/hosts` добавьте запись:

   ```
   <IP_address> <new_fqdn> <fqdn> <hostname>
   ```

   где:

   `<IP_address>` – IP-адрес сервера;

   `<new_fqdn>` – дополнительное имя хоста;

   `<fqdn>` – исходное FQDN;

   `<hostname>` – короткое имя хоста.

   b. На DNS-сервере создайте CNAME-запись, в которой `<new_fqdn>` указывает на `<fqdn>`.

После настройки используйте дополнительное имя для сервисов KUMA с Raft. Исходное имя хоста изменять не нужно.

4. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре KUMA с хостов хранилищ KUMA.

5. Проверьте количество и актуальность источников событий, для которых отображается красный статус, в разделе **Состояние источников** → **Список источников событий** и для неактуальных источников событий выполните одно из следующих действий:

   - удалите неактуальные источники событий;
   - измените параметры политик мониторинга, примененных к неактуальным источникам событий, так, чтобы они соответствовали актуальному потоку событий;
   - для политик мониторинга, примененных к неактуальным источникам событий, отключите рассылку уведомлений.

   После обновления KUMA для всех источников событий с красным статусом, для которых настроена отправка уведомлений о срабатывании политики, будут отправлены уведомления на указанные адреса электронной почты.

Обновление KUMA

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке решения. В файле инвентаря в секции `kuma_metrics` необходимо указать хост, на котором запущен активный сервис Метрики. При запуске обновления выполняется проверка и если сервис Метрики на этом хосте не найден, вернется ошибка и обновление прервется.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации с Ядром KUMA в кластере Kubernetes. В файле инвентаря в секции `kuma_metrics` необходимо указать хост, на котором запущен активный сервис Метрики. При запуске обновления выполняется проверка и если сервис Метрики на этом хосте не найден, вернется ошибка и обновление прервется.

  Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

Процесс обновления полностью повторяет процесс установки.

Вы можете изменить тип установки следующим образом:

- Если вы хотите выполнить обновление с распределенной установки до установки с Ядром KUMA в кластере Kubernetes, выполните обновление распределенной установки до последней версии, а затем выполните **Перенос Ядра в кластер Kubernetes**. Для дальнейшего обновления используйте файл инвентаря k0s.inventory.yml с параметром `need_transfer: false`, поскольку перенос Ядра KUMA в кластер Kubernetes уже выполнен и больше не требуется.

  Чтобы перенести Ядро KUMA в новый кластер Kubernetes, выполните следующие шаги:

  1. Подготовьте файл инвентаря k0s.inventory.yml.

     В файле инвентаря k0s.inventory.yml в разделах kuma_core, kuma_ collector, kuma_correlator, kuma_storage укажите те же хосты, которые использовались при обновлении KUMA с версии 2.1.3 до версии 3.0.3, и затем до версии 3.2, или при новой установке решения. В файле инвентаря необходимо присвоить параметрам deploy_to_k8s и need_transfer значение true. Параметру deploy_example_services необходимо присвоить значение false.

  2. Выполните шаги распределенной установки с использованием подготовленного файла инвентаря k0s.inventory.yml.

Процесс переноса Ядра KUMA в новый кластер Kubernetes

При запуске установщика с файлом инвентаря производится поиск установленного Ядра KUMA на всех хостах, на которых планируется размещать рабочие узлы кластера. Найденное Ядро будет перенесено с хоста внутрь создаваемого кластера Kubernetes.

Если на рабочих узлах компонент не обнаружен, то производится чистая установка Ядра KUMA в кластер без переноса в него ресурсов. Существующие компоненты требуется пересоздать с новым Ядром вручную в веб-интерфейсе KUMA.

Для коллекторов, корреляторов и хранилищ из файла инвентаря будут заново выпущены сертификаты для связи с Ядром внутри кластера. URL Ядра для компонентов при этом не изменится.

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-vmalert.
- Удаляет internal сертификат Ядра.
- Удаляет файлы сертификатов всех прочих компонентов и удаляет записи о них из MongoDB.
- Удаляет директории:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/log
  - /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра KUMA>/logs
  - /opt/kaspersky/kuma/metrics/<идентификатор сервиса Метрики>/bin

- Переносит данные Ядра и ее зависимостей на сетевой диск внутри кластера Kubernetes.
- На хосте с Ядром переносит директории:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

  После проверки корректности переноса Ядра в кластер данные директории можно удалить.

  В случае возникновения проблем с переносом нужно проанализировать в журнале записи задачи переноса core-transfer в пространстве имен kuma на кластере (задача доступна в течение 1 часа после переноса).

  При необходимости повторного переноса необходимо привести названия директорий /opt/kaspersky/kuma/*.moved к их исходному виду.

  Если на хосте с Ядром использовался файл /etc/hosts со строками, не относящимися к адресам 127.X.X.X, при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

- Если вы хотите обновить KUMA в распределенной установке до последней версии KUMA с Ядром в кластере Raft, в файле инвентаря distributed.inventory.yml необходимо вручную добавить группу `kuma_core_peers` и указать в этой группе четное количество серверов, где вы планируете установить дополнительные сервисы Ядра KUMA. Также в группе `kuma_core` и `kuma_core_peers` вы можете указать параметр `raft_node_addr` в формате `<FQDN сервера из группы kuma_core, на котором установлено Ядро KUMA>:<порт>`, если у сервера есть несколько разных FQDN. Указанный в параметре `raft_node_addr` FQDN будет использоваться для прослушивания сигналов от других узлов.

  После запуска установщика с подготовленным файлом инвентаря никакие дополнительные сервисы Ядра KUMA не устанавливаются на серверах автоматически. Установщик только готовит указанные в файле инвентаря серверы к установке сервисов. После завершения работы установщика автоматически установлен только один сервис Ядра KUMA на сервере указанном в группе `kuma_core`. После завершения работы установщика вам необходимо вручную создать сервисы Ядра KUMA в веб-интерфейсе и последовательно установить сервис Ядра KUMA с уникальным идентификатором на каждом сервере, указанном в группе `kuma_core_peers`.

  После обновления все существующие сервисы KUMA будут подключены к Ядру KUMA на сервере из группы `kuma_core`. При дальнейшей установке новых сервисов вы можете указать несколько URL через запятую в команде установки, чтобы подключить сервисы к Ядрам KUMA в кластере Raft.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты KUMA.
3. Для распределенной установки в отказоустойчивой конфигурации с Ядром KUMA в кластере Kubernetes обновите компоненты кластера.

Обновление KUMA успешно выполнено.

Известные ограничения

1. Для действующих пользователей при обновлении с 4.0.x до 4.2 не выполняется обновление универсального макета панели мониторинга.

   Возможное решение: перезапустите сервис Ядра kuma-core-<`идентификатор сервиса Ядра KUMA`>.service - данные будут обновляться с заданным для панели мониторинга интервалом.

Обновление компонентов кластера Kubernetes

Обновление компонентов кластера Kubernetes выполняется только в случае обновления KUMA до версии 4.2.x. При установке KUMA 4.2.x с нуля обновление компонентов кластера Kubernetes не требуется.

> Перед выполнением обновления компонентов кластера Kubernetes вам нужно создать резервную копию Ядра KUMA 4.2 вручную на случай непредвиденных сбоев обновления. Если у вас отсутствует резервная копия Ядра KUMA 4.2, созданная вручную, в случае сбоя все данные могут быть утрачены.

Обновление компонентов кластера Kubernetes выполняется с выделенной машины ansible-controller, не являющейся участником кластера Kubernetes, поскольку скрипт обновления предусматривает перезагрузку всех хостов кластера. Если ansible-controller будет машиной внутри кластера, во время штатной перезагрузки хостов кластера выполнение скрипта прервется и работоспособность кластера будет утрачена.

Обновление компонентов кластера Kubernetes выполняется с помощью скрипта cluster_upgrade.sh и файла инвентаря k0s.inventory.yaml, только на хостах из секции `k0s` файла инвентаря k0s.inventory.yaml. Внешние сервисы KUMA не затрагиваются.

Логика работы скрипта cluster_upgrade.sh

По умолчанию скрипт обновления предусматривает автоматическое создание резервной копии.

Если создание резервной копии Ядра KUMA вручную на случай непредвиденных сбоев обновления заняло значительное время и вы не хотите ждать аналогичное время при автоматическом создании резервной копии, вы можете поместить резервную копию, созданную вручную, на выделенной машине ansible-controller в файл autobackup.tar.gz и запустить скрипт с параметром `-e 'manual_restore_only=true'`. Применение параметра `-e 'manual_restore_only=true'` при запуске скрипта позволяет пропустить этап автоматического создания резервной копии и автоматического восстановления данных из резервной копии и таким образом сократить время обновления. В этом случае вам необходимо будет восстановить Ядро KUMA из резервной копии вручную.

Доступны следующие способы обновления компонентов кластера Kubernetes:

- Обновление компонентов кластера Kubernetes без параметра -e 'manual_restore_only=true'
- Обновление компонентов кластера Kubernetes с параметром -e 'manual_restore_only=true'

Обновление компонентов кластера Kubernetes без параметра -e 'manual_restore_only=true'

Чтобы выполнить обновление компонентов кластера Kubernetes без параметра -e 'manual_restore_only=true':

1. Выполните подготовку к обновлению:

   a. Убедитесь, что выполнено обновление KUMA с версии 4.0.x до 4.2.x с помощью установщика install.sh и файла инвентаря k0s.inventory.yaml.

   b. Подготовьте выделенную машину ansible-controller, с которой вы будете запускать скрипт обновления, и убедитесь, что машина не является участником кластера. Скрипт обновления предусматривает перезагрузку всех хостов кластера. Если ansible-controller будет машиной внутри кластера, во время штатной перезагрузки хостов кластера выполнение скрипта будет прервано и процесс установки новых версий компонентов Kubernetes аварийно завершится.

   c. Убедитесь, что на выделенной машине ansible-controller и на master-controller достаточно свободного дискового пространства для размещения резервной копии.

   d. Создайте резервную копию Ядра KUMA вручную на случай непредвиденных сбоев.

      Данные метрик в резервную копию не входят и в кластер Kubernetes не переносятся. При обновлении компонентов кластера Kubernetes данные метрик будут утрачены.

      Если вам критически важны данные метрик, обратитесь к специалистам Службы технической поддержки перед обновлением компонентов кластера Kubernetes.

   e. Укажите значение параметра `backup_timeout` в файле инвентаря k0s.inventory.yaml в секции `vars`.

2. Выполните обновление:

   a. На выделенной машине ansible-controller перейдите в директорию установщика 4.2 и запустите скрипт cluster_upgrade.sh, передав в качестве параметра имя актуального файла инвентаря k0s.inventory.yaml:

      ```
      ./cluster_upgrade.sh k0s.inventory.yaml
      ```

   b. В консоли командной строки подтвердите наличие резервной копии Ядра KUMA и согласие с выполнением обновления, указав yes.

      В процессе обновления будет автоматически создана резервная копия Ядра KUMA autobackup.tar.gz. Скрипт создает резервную копию Ядра KUMA на машине master-controller в директории /root/k0s/, а затем переносит на выделенную машину ansible-controller, с которой выполняется обновление компонентов Kubernetes, в директорию со скриптом. В процессе автоматического восстановления данных Ядра KUMA в новом кластере Kubernetes также используется директория установщика и директория /root/k0s/ на машине master-controller.

      Из резервной копии в дальнейшем будет автоматически выполнено восстановление Ядра KUMA в новом кластере Kubernetes. Если в процессе обновления произойдет сбой, вы сможете поместить созданную вручную резервную копию в файл autobackup.tar.gz, расположенный на машине ansible-controller в директории со скриптом, и перезапустить скрипт cluster_upgrade.sh.

      Перезапись созданной резервной копии автоматически не выполняется.

Обновление компонентов кластера Kubernetes выполнено.

Восстановление при сбое

Доступны следующие сценарии восстановления в случае сбоя:

- Сбой при обновлении компонентов кластера Kubernetes. Вы можете использовать любой из вариантов восстановления:

  - Поместить созданную вручную резервную копию в файл autobackup.tar.gz, расположенный на машине master-controller в директории со скриптом, и перезапустить скрипт cluster_upgrade.sh. Скрипт примет созданную вручную резервную копию в обработку и продолжит процедуру обновления.

  - Запустить скрипт cluster_upgrade.sh с указанием параметра `-e 'manual_restore_only=true'` и выполнить восстановление вручную.

- Сбой при запуске Ядра KUMA после успешного обновления кластера Kubernetes.

  Если вы хотите, чтобы скрипт автоматически повторил удаление и новую установку кластера, необходимо остановить службу k0s на любом из узлов кластера и удалить на этом узле исполняемый файл k0s. Скрипт будет интерпретировать состояние кластера как неконсистентное и выполнит удаление и установку кластера с использованием ранее созданного файла autobackup.tar.gz.

  Для остановки службы k0s на контроллерах кластера и хостах, совмещающих роли контроллера и рабочего узла, необходимо использовать следующие команды:

  ```
  sudo systemctl stop k0scontroller.service
  sudo rm /usr/bin/k0s
  ```

  Для остановки службы k0s и удаления бинарного файла k0s на выделенных рабочих узлах необходимо использовать следующие команды:

  ```
  sudo systemctl stop k0sworker.service
  sudo rm /usr/bin/k0s
  ```

  Удаление кластера выполняется только после получения корректного файла резервной копии или явного отказа от автоматического резервного копирования и восстановления применением параметра `-e 'manual_restore_only=true'` и согласия на продолжение обновления без выполнения резервного копирования. Если у вас отсутствует резервная копия, созданная вручную, в случае сбоя все данные будут утрачены.

Обновление компонентов кластера Kubernetes с параметром -e 'manual_restore_only=true'

Чтобы выполнить обновление компонентов кластера Kubernetes с параметром -e 'manual_restore_only=true':

1. Выполните подготовку к обновлению:

   a. Убедитесь, что выполнено обновление KUMA с версии 4.0.x до 4.2.x с помощью установщика install.sh и файла инвентаря k0s.inventory.yaml.

   b. Подготовьте выделенную машину ansible-controller, с которой вы будете запускать скрипт обновления, и убедитесь, что машина не является участником кластера. Скрипт обновления предусматривает перезагрузку всех хостов кластера. Если ansible-controller будет машиной внутри кластера, во время штатной перезагрузки хостов кластера выполнение скрипта будет прервано и процесс установки новых версий компонентов Kubernetes аварийно завершится.

c. Убедитесь, что на выделенной машине ansible-controller и на master-controller достаточно свободного дискового пространства для размещения резервной копии.

d. Создайте резервную копию Ядра KUMA вручную на случай непредвиденных сбоев.

   Данные метрик в резервную копию не входят и в кластер Kubernetes не переносятся. При обновлении компонентов кластера Kubernetes данные метрик будут утрачены.

   Если вам критически важны данные метрик, обратитесь к специалистам Службы технической поддержки перед обновлением компонентов кластера Kubernetes.

2. Выполните обновление:

   a. На выделенной машине ansible-controller перейдите в директорию установщика KUMA 4.2 и запустите скрипт cluster_upgrade.sh, передав в качестве параметра имя актуального файла инвентаря k0s.inventory.yaml и указав параметр `-e 'manual_restore_only=true'`:

   ```
   ./cluster_upgrade.sh k0s.inventory.yaml [-e 'manual_restore_only=true']
   ```

   Автоматическое создание резервной копии и автоматическое восстановление из резервной копии отключены. Скрипт удалит старый кластер и создаст новый кластер Kubernetes.

   b. В консоли командной строки подтвердите наличие резервной копии Ядра KUMA и согласие с выполнением обновления, указав `yes`.

   Если у вас отсутствует созданная вручную резервная копия и вы подтвердите удаление кластера, данные будут утрачены.

3. Выполните восстановление Ядра KUMA из резервной копии.

Обновление компонентов кластера Kubernetes выполнено.

Восстановление при сбое

В случае сбоя при обновлении перезапустите скрипт cluster_upgrade.sh и выполните восстановление Ядра KUMA из резервной копии вручную.

Определение размера данных метрик в установке с Ядром KUMA в кластере Kubernetes версии 3.4.x

При обновлении с KUMA 3.4 до 4.0.x следует определить, сколько места на диске занимают данные метрик и оценить, стоит ли переопределять значение параметра `metrics_disk_request` в файле инвентаря k0s.inventory.yml.

Чтобы оценить, сколько места на диске занимают данные метрик в KUMA 3.4:

На целевой машине запустите скрипт get_old_metrics_size.sh с файлом инвентаря k0s.inventory.yml:

```
sudo ./get_old_metrics_size_sh k0s.inventory.yml
```

Никаких изменений в существующую установку скрипт не вносит, в процессе работы скрипта выполняется подключение к мастер-контроллеру кластера для определения имени тома Ядра KUMA и к рабочим узлам кластера для определения размера директории внутри подключенного тома.

В результате будет выполнен поиск томов Ядра KUMA на рабочих узлах кластера и определен размер каталога victoria-metrics в них. Результат выполнения скрипта выводится на экран и сохраняется в журнале log/get_old_metrics_size-YYYYMMDD-HHMMSS.log. В журнале сохраняется сообщение следующего вида:

```
TASK [Print metrics folder size] ********************************************
ok: [kuma-inst-06.avp.ru] => {}
MSG:
Found KUMA Core 3.4.1.53
Found old metrics folder size: 1Gi
Minimum metrics_data_size required to proceed: 3Gi (including 2Gi threshold)
```

В сообщении указаны следующие сведения:

- `Found KUMA Core` — найденная версия Ядра KUMA.
- `Found old metrics folder size` — текущий размер директории victoria-metrics в ГБ.
- `Minimum metrics_data_size required to proceed` — минимально возможный размер тома метрик для миграции с версии 3.4.x. В этот размер заложен дополнительный запас свободного места в 2Gi. При необходимости вы можете отфильтровать вывод по строке `Minimum metrics_data_size required to proceed`.

По результатам полученных данным вам необходимо определить необходимый размер тома сервиса Метрики в KUMA 4.0.x, в зависимости от ваших потребностей. Размер тома для сервиса Метрики не должен быть меньше значения `Minimum metrics_data_size required to proceed`.

Если при обновлении с версии 3.4.x до версии 4.0.x вы укажете в файле инвентаря k0s.inventory.yml размер тома меньше, чем в `Minimum metrics_data_size required to proceed` или используете значение параметра `metrics_disk_request` которое будет меньше значения `Minimum metrics_data_size required to proceed`, установщик прервет выполнение обновления с версии 3.4.x до версии 4.0.x на этапе валидации установки со следующим сообщением:

```
TASK [Check metrics volume size requirement] ***********************************
fatal: [kuma-inst-06.avp.ru]: FAILED! => {
"changed": false
}
MSG:
Current metrics folder size: 20Gi
Metrics disk request when low_resources=false: 10Gi
Metrics disk request when low_resources=true: 10Gi
Error: Available metric data exceeds specified volume size.
The available metric data (20Gi + 2Gi threshold) is too large.
Solution: Increase the metrics volume size by updating the metrics_disk_request variable in your inventory file.
```

В приведенном примере пользователь попытался задать размер тома 10Gi через переменную инвентаря metrics_disk_request, при этом текущий размер данных метрик на диске - 20Gi. В результате желаемое значение размера тома меньше, чем текущий размер данных + порог в 2Gi, поэтому выполнить обновление с 3.4.x невозможно. Установка будет прервана на шаге валидации, при этом никаких изменений в текущую установку не вносится. Можно безопасно выбрать подходящее значение размера тома для метрик, переопределить его в файле инвентаря и повторить попытку обновления.

Увеличение размера тома Ядра KUMA или тома сервиса Метрики в действующем кластере Kubernetes

В процессе эксплуатации KUMA может потребоваться увеличить размер тома для Ядра KUMA или сервиса Метрики.

Перед увеличением размера томов нужно убедиться, что на рабочих узлах кластера достаточно свободного места в каталоге /opt. Должно быть доступно как минимум вдвое больше свободного места от планируемого размера томов.

Начиная с версии KUMA 4.0.1 в установщик включен скрипт roles/k0s_prepare/files/k0s-pvc-expand.sh, который в процессе установки копируется на мастер-контроллер кластера в директорию /root/k0s/. Этот скрипт позволяет увеличить размер тома в действующем кластере.

Увеличение размера тома с помощью скрипта k0s-pvc-expand.sh

Вы можете увеличить размер тома одним из следующих способов:

- Перейти в директорию /root/k0s/ мастер-контроллера и запустить скрипт k0s-pvc-expand.sh с параметром `core` или `metrics` в зависимости от того, над каким томом будет выполняться действие, и указать новый размер тома в гигабайтах. Размер тома должен быть целым числом без суффикса.

- Вручную скопировать скрипт k0s-pvc-expand.sh на любой контроллер кластера в удобную для запуска директорию и запустить выполнение скрипта.

Пример команды для увеличения размера тома сервиса Метрики до 100 ГБ:

```
sudo ./k0s-pvc-expand.sh metrics 100
```

Пример увеличения размера тома Ядра KUMA до 200 ГБ:

```
sudo ./k0s-pvc-expand.sh core 200
```

Поведение скрипта

Если задаваемый размер тома меньше или равен текущему, никакие действия выполняться не будут и скрипт прервет свою работу и вернет сообщение об ошибке.

Если желаемый размер тома больше текущего, в процессе выполнения скрипт остановит сервис, использующий том: Ядро KUMA или сервис Метрики. После отключения тома от подов сервиса скрипт проведет увеличение размера тома. После изменения размера тома сервис будет вновь запущен и сможет использовать увеличенный том.

После увеличения размера тома для обновления на более поздние версии KUMA никаких дополнительных указаний размера томов в инвентаре не понадобится - установщик KUMA будет использовать текущие размеры томов и будет игнорировать отличные от них значения переменных из файла инвентаря.

Уменьшение размера тома сервиса Метрики

Перед уменьшением тома сервиса Метрики вам необходимо определить достаточный размер тома, опираясь на метрики в разделе **Метрики** → **Сервис Метрики KUMA** → **Хранилище** → **Использование дискового пространства**. Следует учитывать длительность хранения метрик и создавать запас дискового пространства, если планируется увеличение числа источников метрик.

Перед уменьшением томов следует убедиться, что задача metrics-transfer-<уникальный идентификатор> отсутствует.

```
k0s kubectl get jobs -n kuma
```

Вывод команды должен быть `"No resources found in kuma namespace."`. Задача metrics-transfer будет самостоятельно удалена через 1 час после завершения.

Если требуется удалить ее раньше, можно воспользоваться командой:

```
k0s kubectl delete job metrics-transfer -n kuma
```

Вы можете выполнить уменьшение размера тома одним из следующих способов:

- Уменьшение размера тома сервиса Метрики без потери данных.
- Уменьшение размера тома сервиса Метрики с потерей данных.

Уменьшение размера тома сервиса Метрики без потери данных

Чтобы уменьшить размер тома сервиса Метрики без потери данных:

1. Отмонтируйте том сервиса Метрики:

   a. Получите имя тома, используемого сервисом Метрики. В дальнейшем имя тома понадобится для поиска данных тома и реплик тома. Имена реплик начинаются с имени тома.

   ```
   sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
   ```

   b. Останавите сервис Метрики.

   ```
   sudo k0s kubectl scale deployment/metrics -n kuma --replicas=0
   ```

   c. Убедитесь, что под сервиса Метрики metrics-<UID> пропал (отсутствует в выводе команды).

   ```
   sudo k0s kubectl get pods -n kuma
   ```

   d. Если под не пропадает в течение нескольких минут, выполните принудительное удаление. Имя пода нужно взять из вывода предыдущей команды.

   ```
   sudo k0s kubectl delete pod metrics-<UID> -n kuma --force
   ```

   e. Убедитесь, что том сервиса Метрики перешел в состояние detached.

   ```
   sudo k0s kubectl get volume <имя_тома> -n longhorn-system -o json | jq
   '.status.state'
   ```

2. Создайте временную задачу:

   a. Создайте временную задачу с именем tmp-metrics-job в пространстве имен kuma и подключите том сервиса Метрики.

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: batch/v1
kind: Job
metadata:
  name: tmp-metrics-job
  namespace: kuma
spec:
  ttlSecondsAfterFinished: 300
  backoffLimit: 0
  parallelism: 1
  completions: 1
  template:
    spec:
      containers:
        - name: tmp-container
          image: docker.io/library/busybox:1.35.0
          imagePullPolicy: IfNotPresent
          command: ["/bin/sh"]
          args:
            - -c
            - >-
                sleep 36000
          volumeMounts:
            - mountPath: /metrics
              name: metrics
      restartPolicy: Never
      volumes:
        - name: metrics
          persistentVolumeClaim:
            claimName: metrics
EOF
```

   b. Определите имя рабочего узла, на котором запущена временная задача.

```
sudo k0s kubectl get pods -n kuma -o wide | grep tmp-metrics
```

   c. На этом рабочем узле определите точку монтирования.

```
sudo lsblk | grep "<имя_тома>"
```

   d. Перейдите в найденную директорию вида /var/lib/k0s/kubelet/pods/...../mount. Содержимое выглядит примерно следующим образом:

```
ls -al
total 48
drwxrwsr-x 9 root  65532  4096 Aug 26 10:36 .
drwxr-x--- 3 root  root   4096 Aug 26 11:08 ..
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 certificates
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 dashboards
drwxrwsr-x 8 root  65532  4096 Aug 26 10:34 data
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 log
drwxrws--- 2 root  65532 16384 Aug 26 10:34 lost+found
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 rules
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 tmp
```

3. Копируйте данные:

   a. Копируйте из директории вида /var/lib/k0s/kubelet/pods/...../mount все данные, кроме каталогов lost+found и tmp во временную директорию с сохранением прав доступа на каталоги и файлы.

   b. После копирования перейдите из точки монтирования в / или /home, чтобы не блокировать последующее демонтирование тома.

4. Удалите временную задачу, под, PVC и том сервиса Метрики:

   a. Удалите временную задачу с помощью следующей команды:

   ```
   sudo k0s kubectl delete job tmp-metrics-job -n kuma
   ```

   b. Убедитесь, что под временной задачи metrics-<UID> отсутствует в выводе команды.

   ```
   sudo k0s kubectl get pods -n kuma
   ```

   c. Если под не пропадает в течение нескольких минут, выполните принудительное удаление. Имя пода нужно взять из вывода предыдущей команды.

   ```
   sudo k0s kubectl delete pod tmp-metrics-job-<UID> -n kuma --force
   ```

   d. Убедитесь, что том сервиса Метрики перешел в состояние detached.

   ```
   sudo k0s kubectl get volume <имя_тома> -n longhorn-system -o json | jq
   '.status.state'
   ```

   e. Удалите PVC сервиса Метрики.

   ```
   sudo k0s kubectl delete pvc metrics -n kuma
   ```

   f. Убедитесь, что том сервиса Метрики отсутствует в выводе команды.

   ```
   sudo k0s kubectl get volume <имя_тома> -n longhorn-system
   ```

   На всех рабочих узлах при этом в директории /opt/longhorn/replicas должны пропасть директории, имя которых начинается с имени удаленного тома. Если этого не произошло, то их нужно удалить вручную. Важно не удалить по ошибке реплики, относящиеся к другим томам.

5. Создайте новый том:

   a. Создайте PVC для сервиса Метрики, предварительно исправив размер в строке storage на нужное значение.

   ```
   sudo k0s kubectl apply -f - <<EOF
   ---
   apiVersion: v1
   kind: PersistentVolumeClaim
   metadata:
     name: metrics
     namespace: kuma
   spec:
     accessModes:
       - ReadWriteOnce
     storageClassName: kuma-network-storage
     resources:
       requests:
         storage: 30Gi
   EOF
   ```

b. Заново получите имя тома, используемого сервисом Метрики.

```
sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
```

c. Снова создайте временную задачу с именем tmp-metrics-job в пространстве имен kuma и подключите новый том сервиса Метрики.

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: batch/v1
kind: Job
metadata:
  name: tmp-metrics-job
  namespace: kuma
spec:
  ttlSecondsAfterFinished: 300
  backoffLimit: 0
  parallelism: 1
  completions: 1
  template:
    spec:
      containers:
        - name: tmp-container
          image: docker.io/library/busybox:1.35.0
          imagePullPolicy: IfNotPresent
          command: ["/bin/sh"]
          args:
            - -c
            - >-
                sleep 36000
          volumeMounts:
            - mountPath: /metrics
              name: metrics
      restartPolicy: Never
      volumes:
        - name: metrics
          persistentVolumeClaim:
            claimName: metrics
EOF
```

d. Определите имя рабочего узла, на котором запущена временная задача.

```
sudo k0s kubectl get pods -n kuma -o wide | grep tmp-metrics
```

e. На этом рабочем узле определите точку монтирования.

```
sudo lsblk | grep "<имя_тома>"
```

f. Перейдите в найденную директорию вида /var/lib/k0s/kubelet/pods/……/mount.

6. Копируйте данные:

a. Копируйте в найденную директорию вида /var/lib/k0s/kubelet/pods/……/mount ранее сохраненные во временной директории данные сервиса Метрики с сохранением владельцев и прав файлов. В результате содержимое директории будет примерно следующим.

```
ls -al
total 48
drwxrwsr-x 9 root  65532  4096 Aug 26 10:36 .
drwxr-x--- 3 root  root   4096 Aug 26 11:08 ..
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 certificates
```

```
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 dashboards
drwxrwsr-x 8 root  65532  4096 Aug 26 10:34 data
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 log
drwxrws--- 2 root  65532 16384 Aug 26 10:34 lost+found
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 rules
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 tmp
```

b. После копирования перейдите из точки монтирования в / или /home, чтобы не блокировать последующее демонтирование тома.

7. Удалите временную задачу, под, PVC и том сервиса Метрики:

a. Удалите временную задачу с помощью следующей команды.

```
sudo k0s kubectl delete job tmp-metrics-job -n kuma
```

b. Убедитесь, что под временной задачи metrics-<UID> отсутствует в выводе команды.

```
sudo k0s kubectl get pods -n kuma
```

c. Если под не пропадает в течение нескольких минут, выполните форсированное удаление. Имя пода нужно взять из вывода предыдущей команды.

```
sudo k0s kubectl delete pod tmp-metrics-job-<UID> -n kuma --force
```

d. Убедитесь, что том сервиса Метрики перешел в состояние detached.

```
sudo k0s kubectl get volume <имя_тома> -n longhorn-system -o json | jq
'.status.state'
```

8. Запустите сервис Метрики:

a. Запустите сервис Метрики с помощью следующей команды, увеличив число реплик до 1.

```
sudo k0s kubectl scale deployment/metrics -n kuma --replicas=1
```

b. Убедитесь, что под сервиса Метрики запущен и метрики доступны в веб-интерфейсе KUMA.

Уменьшение размера тома сервиса Метрики без потери данных выполнено.

Уменьшение размера тома сервиса Метрики с потерей данных

Чтобы уменьшить размер тома сервиса Метрики с потерей данных:

1. Получите имя тома, используемого сервисом Метрики. В дальнейшем имя тома понадобится для поиска данных тома и реплик тома. Имена реплик начинаются с имени тома.

```
sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
```

2. Остановите сервис Метрики.

```
sudo k0s kubectl scale deployment/metrics -n kuma --replicas=0
```

3. Убедитесь, что под сервиса Метрики metrics-<UID> отсутствует в выводе команды.

```
sudo k0s kubectl get pods -n kuma
```

4. Если под не пропадает в течение нескольких минут, выполните форсированное удаление. Имя пода нужно взять из вывода предыдущей команды.

   ```
   sudo k0s kubectl delete pod metrics-<UID> -n kuma --force
   ```

5. Убедитесь, что том сервиса Метрики перешел в состояние detached.

   ```
   sudo k0s kubectl get volume <имя_тома> -n longhorn-system -o json | jq '.status.state'
   ```

6. Удалите PVC сервиса Метрики.

   ```
   sudo k0s kubectl delete pvc metrics -n kuma
   ```

7. Убедитесь, что том сервиса Метрики отсутствует в выводе команды.

   ```
   sudo k0s kubectl get volume <имя_тома> -n longhorn-system
   ```

   На всех рабочих узлах в директории /opt/longhorn/replicas должны пропасть директории, имя которых начинается с имени удаленного тома. Если этого не произошло, то их нужно удалить вручную. Важно не удалить по ошибке реплики, относящиеся к другим томам.

8. Создайте PVC для сервиса Метрики, предварительно исправив размер в строке storage на нужное значение.

   ```
   sudo k0s kubectl apply -f - <<EOF
   ---
   apiVersion: v1
   kind: PersistentVolumeClaim
   metadata:
     name: metrics
     namespace: kuma
   spec:
     accessModes:
       - ReadWriteOnce
     storageClassName: kuma-network-storage
     resources:
       requests:
         storage: 30Gi
   EOF
   ```

9. Запустите сервис Метрики, увеличив число реплик до 1.

   ```
   sudo k0s kubectl scale deployment/metrics -n kuma --replicas=1
   ```

10. Убедитесь, что под сервиса Метрики запущен и метрики доступны в веб-интерфейсе KUMA.

Уменьшение размера тома сервиса Метрики с потерей данных выполнено.

Миграция событий алертов в ClickHouse после обновления KUMA с версии 3.4.x

После обновления KUMA с версии 3.4.x до версии 4.0 необходимо выполнить миграцию событий алертов из MongoDB в ClickHouse и указать хранилище в параметрах наполнения алертов.

После обновления KUMA установщик останавливает сервис kuma-mongodb, который затем нужно вручную запустить перед миграцией событий алертов. Если Ядро KUMA развернуто в кластере Kubernetes, после обновления контейнер с MongoDB также не будет запущен, поэтому его потребуется запустить перед миграцией.

Если вам необходимо прервать выполнение команды для миграции событий алертов, нажмите **`Ctrl+C`** в консоли командной строки. Отобразится уведомление о том, что команда будет остановлена. Текущая пачка событий будет безопасно перенесена в хранилище, прогресс миграции сохранится, и процесс можно будет продолжить при следующем запуске команды.

Миграция событий алертов доступна для следующих типов установки:

- KUMA в неотказоустойчивой конфигурации.
- Распределенная установка с Ядром KUMA в кластере Kubernetes.

Миграция событий алертов в случае обновления KUMA в неотказоустойчивой конфигурации

Чтобы выполнить миграцию событий алертов в неотказоустойчивой конфигурации:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** выберите хранилище, в которое будут перенесены события алертов, и нажмите **Копировать идентификатор кластера**. Идентификатор кластера хранения понадобится при выполнении команды по переносу событий алертов.

2. На сервере с Ядром KUMA запустите сервис kuma-mongodb.service с помощью следующей команды:

   ```
   sudo systemctl start kuma-mongodb.service
   ```

3. Перейдите в директорию /opt/kaspersky/kuma и выполните следующую команду, подставив нужные значения в параметры и подставив скопированный ранее идентифкатор кластера хранения в параметр `--cluster-id`:

   ```
   ./kuma tools migrate --mongo="mongodb://<имя хоста, на котором установлена MongoDB>:<порт>" --core-url="https://<FQDN сервера, на котором установлено Ядро KUMA>:<порт>" --core-dir="<директория хранения данных Ядра KUMA: в зависимости от типа установки /opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000 или /opt/kaspersky/kuma/core>" --cluster-id="<идентификатор кластера хранения, куда вы хотите перенести события алертов KUMA 3.4>" --batch=<количество событий алертов в пачке> 2>&1 | tee /tmp/migrate.log | grep -v "debug"
   ```

   Пример:

   ```
   ./kuma tools migrate --mongo="mongodb://localhost:27017" --core-url="https://kuma.example.com:7210" --core-dir="/opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000" --cluster-id="0a123456-789a-0123-ab12-a3fab45ab6a7" --batch=10000 2>&1 | tee /tmp/migrate.log | grep -v "debug"
   ```

   Доступные параметры миграции событий алертов из MongoDB в ClickHouse

   Полный вывод команды будет сохранен в файл /tmp/migrate.log.

   Миграция может занять продолжительное время, если алертов много. Чтобы ускорить процесс миграции, вы можете применить параметр `--batch`, предварительно выделив дополнительное дисковое пространство и ОЗУ. Например, 150 000 алертов можно перенести за одну итерацию длительностью около трех минут при ОЗУ 12 ГБ для мигратора и MongoDB и дисковом пространстве 30 ГБ при значении параметра `--batch` равном `150000`. В этом примере значения и продолжительность миграции приведены в качестве ориентира. Продолжительность может отличаться в зависимости от количества алертов и событий в алертах, от доступного дискового пространства и ОЗУ, а также от количества событий алертов в пачке, указанном в параметре `--batch`. Вы можете адаптировать значения под свои нужды.

   Также вы можете ускорить миграцию, если хотите перенести только часть событий алертов, например, только события алертов за последний год. В таком случае вы можете указать значение параметра `--time-limit`, который будет соответствовать значению параметра **Срок хранения алертов, дни**.

Например, у вас есть события алертов за полтора года, а вы хотите выполнить миграцию события алертов за последний год. Вы выполняете миграцию 18 августа 2025 года, при этом для параметра **Срок хранения алертов, дни** указано значение **365**, тогда в значении параметра `--time-limit` следует указать 19 августа 2024 года следующим образом: `--time-limit="Sun, 19 Aug 2024 00:01:00 UTC"`.

В ходе миграции будут перенесены только события алертов за последние 365 дней. Это позволит ускорить миграцию и избежать переноса лишних событий.

Если вы не укажете значение параметра `--time-limit`, будет выполнена миграция всех событий алертов в ClickHouse, но это может занять больше времени, а события алертов старше заданного срока хранения алертов будут позднее удалены из ClickHouse.

4. После выполнения команды остановите сервис mongodb и отключите его запуск следующими командами:

```
sudo systemctl stop kuma-mongodb.service
sudo systemctl disable kuma-mongodb.service
```

Перенос событий алертов выполнен.

> После обновления KUMA и переноса событий алертов хранилище для новых событий алертов не указывается автоматически. Вы указали кластер хранения только для переноса существующих событий алертов. Чтобы новые алерты наполнялись событиями, необходимо вручную указать значение параметра **Хранилище** в параметрах наполнения алертов. Пока значение параметра не будет указано, все новые алерты будут создаваться без событий.

Миграция событий алертов после обновления KUMA с Ядром KUMA в кластере Kubernetes

Чтобы выполнить перенос событий алертов в KUMA с Ядром KUMA в кластере Kubernetes:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** выберите хранилище, куда будут перенесены события алертов, и нажмите **Копировать идентификатор**. Идентификатор кластера хранения понадобится при выполнении команды по переносу событий алертов.

2. Запустите контейнер с MongoDB в поде Ядра KUMA, выполнив следующую команду на мастер-контроллере:

```
sudo k0s kubectl apply -f /root/k0s/core-manifest.yaml
```

Будет выполнен перезапуск Ядра KUMA.

3. Подключитесь к мастер-контроллеру кластера k0s и запустите перенос событий алертов, подставив в команду полученный ранее идентифкатор кластера хранения в параметр `--cluster-id`:

```
k0s kubectl exec -it deployment/core-deployment -c core -n kuma -- kuma tools migrate
--mongo="mongodb://127.0.0.1:27017" --core-url="https://core:7210" --core-
dir="/opt/kaspersky/kuma/core" --cluster-id="ec9e34bc-8c05-4f95-bb37-cfd5fe4b354a" --
wd="/opt/kaspersky/kuma/core" --batch=10000 2>&1 | tee /tmp/migrate.log | grep -v
"debug"
```

Доступные параметры миграции событий алертов из MongoDB в ClickHouse

Полный вывод команды будет сохранен в файл /tmp/migrate.log на хосте, где вы запускаете `k0s kubectl`, а не в томе пода.

Миграция может занять продолжительное время, если алертов много. Если прервется ssh-сессия, команда продолжит выполняться на поде. В таком случае запускать команду повторно не нужно. Можно отследить выполнение команды в процессах на рабочем узле где запущено Ядро KUMA:

```
sudo watch 'ps -faux | grep "kuma tools migrate"'
```

Чтобы ускорить процесс миграции, вы можете применить параметр `--batch`, предварительно выделив дополнительное дисковое пространство и ОЗУ. Например, 150 000 алертов можно перенести за одну итерацию длительностью порядка трех минут при ОЗУ 12 ГБ для мигратора и MongoDB и дисковом пространстве 30 ГБ при значении параметра `--batch` равном 150000. В этом примере значения и продолжительность миграции приведены в качестве ориентира. Продолжительность может отличаться в зависимости от количества алертов и событий в алертах, от доступного дискового пространства и ОЗУ и от количества событий алертов в пачке, указанном в параметре `--batch`. Вы можете адаптировать значения под свои нужды.

Также вы можете ускорить миграцию, если хотите перенести только часть событий алертов, например, только события алертов за последний год. В таком случае вы можете указать значение параметра `--time-limit`, который будет соответствовать значению параметра **Срок хранения алертов, дни**.

Например, у вас есть события алертов за полтора года, а вы хотите выполнить миграцию событий алертов за последний год. Вы выполняете миграцию 18 августа 2025 года, при этом для параметра **Срок хранения алертов, дни** указано значение **365**, тогда в значении параметра `--time-limit` следует указать 19 августа 2024 года следующим образом: `--time-limit="Sun, 19 Aug 2024 00:01:00 UTC"`.

В ходе миграции будут перенесены только события алертов за последние 365 дней. Это позволит ускорить миграцию и избежать переноса лишних событий.

Если вы не укажете значение параметра `--time-limit`, миграция всех событий алертов в ClickHouse будет выполнена, но это может занять больше времени, а события алертов старше заданного срока хранения алертов будут позднее удалены из ClickHouse.

4. После успешного переноса событий алертов мы рекомендуем запустить Ядро KUMA без контейнера MongoDB. Для этого на мастер-контроллере выполните запуск Ядра KUMA в версии без контейнера MongoDB с помощью следующей команды:

   ```
   sudo k0s kubectl apply -f /root/k0s/core-manifest-no-mongodb.yaml
   ```

   Будет выполнен перезапуск Ядра KUMA.

Перенос событий алертов выполнен.

> После обновления KUMA и переноса событий алертов хранилище для новых событий алертов не указывается автоматически. Вы указали кластер хранения только для переноса существующих событий алертов. Чтобы новые алерты наполнялись событиями, необходимо вручную указать значение параметра **Хранилище** в параметрах наполнения алертов. Пока значение параметра не будет указано, все новые алерты будут создаваться без событий.

После миграции событий алертов в KUMA 4.0 нужно учитывать особенности их резервного копирования и восстановления такой резервной копии с помощью REST API.

Параметры миграции событий алертов из MongoDB в ClickHouse

В таблице ниже приведены доступные параметры миграции событий алертов из MongoDB в ClickHouse и их описание.

Доступные параметры миграции событий алертов из MongoDB в ClickHouse

Параметр	Тип	Описание	Значение по умолчанию
`--batch`	int	Размер пачки событий, которая будет полностью перенесена в хранилище за одну итерацию миграции. Увеличение значения позволяет ускорить миграцию, но требует большего расхода оперативной и дисковой памяти. Значение параметра следует определять, исходя из общего количества алертов и доступных ресурсов. Чтобы узнать общее количество алертов, перейдите в раздел **Алерты** и в раскрывающемся списке **Фильтры** нажмите **Очистить фильтры**. Общее количество алертов отобразится в поле **Найдено**.	100
`--cluster-id`	string	Идентификатор кластера для хранения событий алертов. Идентификатор кластера можно получить в веб-интерфейсе KUMA в разделе **Активные сервисы**. Для этого выберите хранилище для миграции событий алертов, правой кнопкой мыши откройте контекстное меню и выберите **Копировать идентификатор**.	–
`--core-dir`	string	Рабочая директория Ядра KUMA с идентификатором сервиса. Здесь располагается папка с сертификатами.	–
`--core-url`	string	URL внутреннего API Ядра KUMA. По умолчанию API доступно на порту 7210.	–
`--mongo`	string	URL MongoDB для подключения. Здесь хранятся события алертов, которые требуется мигрировать.	"mongodb://localhost:27017"
`--time-limit`	string	Параметр позволяет выполнить миграцию событий алертов, созданные в период от указанной временной метки (в формате RFC1123) до текущего момента. Мы рекомендуем учитывать значение параметра **Срок хранения алертов, дни**, поскольку события алертов старше срока хранения алертов будут удалены из ClickHouse после миграции. Пример: У вас есть события алертов за полтора года, а вы хотите выполнить миграцию только части событий алертов, например только за последний год. Если вы выполняете миграцию 18 августа 2025 года, при этом для параметра **Срок хранения алертов, дни** указано значение **365**, тогда в значении параметра `--time-limit` следует указать 19 августа 2024 года следующим образом: `--time-limit="Sun, 19 Aug 2024 00:01:00 UTC"`. В результате при миграции будут перенесены только события алертов за последние 365 дней. Это позволит ускорить миграцию и избежать переноса лишних событий. Если вы не укажете значение параметра `--time-limit`, миграция всех событий алертов в ClickHouse будет выполнена, но это может занять больше времени, а события алертов старше заданного срока хранения алертов будут позднее удалены из ClickHouse.	–
`--timeout`	int	Время ожидания соединения с хранилищем ClickHouse в секундах.	10
`--wd`	string	Рабочая директория команды `migrate`. Служит для хранения временных и служебных файлов команды. У процесса должны быть права на запись в эту директорию. Обязательный параметр для установки с Ядром KUMA в кластере Kubernetes. Если параметр не задан, в качестве служебной директории будет использоваться текущая рабочая директория, из которой запускается команда.	–

Устранение ошибок при обновлении

При обновлении KUMA вы можете столкнуться со следующими ошибками:

- **Ошибка времени ожидания**

  При обновлении с версии 2.0.x на системах, которые содержат большие данные и при этом работают на предельных ресурсах, после того, как вы введете пароль администратора, система может вернуть сообщение об ошибке `Wrong admin password`. Если вы указываете верный пароль, KUMA может все равно возвращать ошибку, потому что из-за предельных ресурсов и ошибки времени ожидания KUMA не удалось запустить сервис Ядра KUMA. Если вы введете пароль администратора трижды, не дожидаясь завершения установки, обновление может завершиться фатальной ошибкой.

Чтобы устранить ошибку времени ожидания и успешно завершить обновление:

1. Откройте отдельный второй терминал и запустите следующую команду, чтобы убедиться, что вывод команды содержит строку с сообщением об ошибке времени ожидания:

   ```
   journalctl -u kuma-core | grep 'start operation timed out'
   ```

   Сообщение об ошибке времени ожидания:

   `kuma-core.service: start operation timed out. Terminating.`

2. После того как вы нашли сообщение об ошибке времени ожидания, в файле сервиса `/usr/lib/systemd/system/kuma-core.service` измените значение параметра `TimeoutSec` с 300 на 0, чтобы снять ограничения по времени ожидания и временно исключить возможность повторного появления ошибки.

3. После изменения файла сервиса последовательно выполните следующие команды:

   ```
   systemctl daemon-reload
   ```

   ```
   service kuma-core restart
   ```

4. После выполнения команд и успешного запуска сервиса во втором терминале еще раз введите пароль администратора в исходном первом терминале, где установщик запрашивает пароль.

   KUMA продолжит установку. В условиях предельных ресурсов установка может занять до часа.

5. После успешного завершения установки верните параметр `TimeoutSec` к значению 300 в файле `/usr/lib/systemd/system/kuma-core.service`.

6. После изменения файла сервиса выполните следующие команды во втором терминале:

   ```
   systemctl daemon-reload
   ```

   ```
   service kuma-core restart
   ```

После выполнения команд обновление будет успешно выполнено.

- **Неверный пароль администратора**

  Пароль к пользователю admin нужен для автоматического заполнения параметров хранилища при обновлении. Если при выполнении задачи `TASK [Prompt for admin password]` вы указали неверный пароль к пользователю admin девять раз, установщик все равно выполнит обновление и веб-интерфейс будет доступен, но параметры хранилища не мигрируют и хранилища будут в красном статусе.

Чтобы устранить ошибку и сделать хранилища вновь доступными для работы, обновите настройки хранилища:

1. Перейдите в параметры хранилища, вручную заполните поля кластера ClickHouse и нажмите **Сохранить**.
2. Перезапустите сервис хранилища.

   Сервис хранилища будет запущен с заданными параметрами и будет в зеленом статусе.

- **Ошибка DB::Exception**

  После обновления KUMA хранилище может быть в красном статусе, а в его журналах могут отображаться ошибки.

  Пример ошибки:

  ```
  DB::Exception::Exception(std::__1::basic_string<char, std::__1::char_traits<char>,
  std::__1::allocator<char>> const&, int, bool) @ 0xda0553a in
  /opt/kaspersky/kuma/clickhouse/bin/clickhouse
  ```

  Чтобы перезапустить ClickHouse, выполните следующую команду на сервере хранилища KUMA:

  ```
  touch /opt/kaspersky/kuma/clickhouse/data/flags/force_restore_data && systemctl restart kuma-storage-
  <идентификатор хранилища, в котором обнаружена ошибка>
  ```

Устраните ошибки, чтобы успешно завершить обновление.

Перевыпуск сертификатов кластера k0s при истечении срока действия

Проблема

Невозможно подключить контроллеры или рабочие узлы, перенести поды с одного рабочего узла на другой.

В журналах сервисов `k0scontroller` и `k0sworker` появляются множественные записи со следующей подстрокой:

```
x509: certificate has expired or is not yet valid
```

Причина

Срок действия служебных сертификатов кластера при создании составляет 1 год. Используемый в отказоустойчивой конфигурации KUMA кластер k0s обеспечивает автоматическую ротацию всех необходимых ему служебных сертификатов, но ротация производится только при запуске сервиса `k0scontroller`. Если службы `k0scontroller` на контроллерах кластера работают без перезапуска больше 1 года, то служебные сертификаты становятся недействительными.

Способ исправления

Чтобы исправить ошибку, поочередно перезапустите сервисы `k0scontroller` *с правами root на каждом контроллере кластера:*

```
systemctl restart k0scontroller
```

Сертификаты будут перевыпущены.

Чтобы проверить сроки действия сертификатов на контроллерах, выполните следующие команды с правами root:

```
find /var/lib/k0s/pki/ -type f -name "*.crt" -print|egrep -v 'ca.crt$'|xargs -L 1 -t  -i bash -c 'openssl x509  -
noout -text -in {}|grep After'
```

```
find /var/lib/k0s/pki/etcd -type f -name "*.crt" -print|egrep -v 'ca.crt$'|xargs -L 1 -t  -i bash -c 'openssl x509
-noout -text -in {}|grep After'
```

Команды выведут названия файлов сертификатов и сроки их действия.

Удаление KUMA

При удалении KUMA используется инструмент Ansible и созданный пользователем файл инвентаря.

Чтобы удалить KUMA:

1. На контрольной машине войдите в директорию установщика:

   ```
   cd kuma-ansible-installer
   ```

2. Выполните следующую команду:

   ```
   sudo ./uninstall.sh <файл инвентаря>
   ```

   KUMA и все данные решения удалены с серверов.

Базы данных, которые использовались KUMA (например, база данных хранилища ClickHouse), и содержащуюся в них информацию следует удалить отдельно.

Особенности удаления KUMA, установленной в отказоустойчивом варианте

Состав удаляемых компонентов зависит от значения параметра `deploy_to_k8s` в файле инвентаря, используемого для удаления KUMA:

- `true` – удаляется созданный при установке KUMA кластер Kubernetes.
- `false` – из кластера Kubernetes удаляются все компоненты KUMA, кроме Ядра. Сам кластер не удаляется.

Помимо установленных вне кластера компонентов KUMA на узлах кластера удаляются следующие директории и файлы:

- /usr/bin/k0s
- /etc/k0s/
- /var/lib/k0s/
- /usr/libexec/k0s/
- ~/k0s/ (для пользователя ansible_user)
- /opt/longhorn/
- /opt/cni/
- /opt/containerd

При удалении кластера возможен вывод на экран сообщений об ошибках, при котором работа установщика не прерывается.

- Для задач **Delete KUMA transfer job** и **Delete KUMA pod** такие сообщения можно игнорировать.
- Для задач **Reset k0s** (при сообщении об ошибке, содержащем текст "`To ensure a full reset, a node reboot is recommended.`") и Delete k0s Directories and files (при сообщении об ошибке, содержащем текст "`Ошибка ввода/вывода: '/var/lib/k0s/kubelet/plugins/kubernetes.io/csi/driver.longhorn.io/`") рекомендуется перезагрузить хост, к которому относится ошибка и выполнить повторное удаление KUMA с тем же файлом инвентаря.

После удаления KUMA необходимо перезагрузить хосты, на которых были установлены компоненты KUMA или Kubernetes.

Работа с тенантами

Доступ к тенантам регулируется в параметрах настройки пользователей. *Главный администратор* имеет доступ к данным всех тенантов. Только пользователь с этой ролью может создавать и удалять тенанты.

Тенанты отображаются в таблице раздела веб-интерфейса KUMA **Параметры** → **Доступ** →**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.

Чтобы создать тенант:

1. В разделе веб-интерфейса KUMA **Параметры** → **Доступ** →**Тенанты** нажмите **Добавить**.

   Откроется окно **Добавить тенант**.

2. В поле **Название** укажите название тенанта. Название должно содержать от 1 до 128 символов в кодировке Unicode.
3. В поле **Ограничение EPS** укажите квоту EPS для тенанта. Поле не является обязательным. Сумма квот EPS для всех тенантов не должна превышать доступное количество EPS по лицензии. Однако KUMA не проверяет значения, введенные в это поле.
4. При необходимости добавьте **Описание** тенанта. Описание должно содержать не более 256 символов в кодировке Unicode.
5. Нажмите **Создать**.

Тенант будет добавлен. Нажмите F5, чтобы обновить страницу. После обновления страницы созданный тенант отобразится в веб-интерфейсе.

Чтобы удалить тенант:

1. В разделе веб-интерфейса KUMA **Параметры** → **Доступ** →**Тенанты** выберите нужный тенант, установив рядом флажок, и затем в панели инструментов выберите **Удалить**.
2. В появившемся окне **Удалить тенант** будет указана информация о тенанте и будет предложено ввести код и подтвердить удаление тенанта. Если хотите продолжить удаление тенанта, введите код.
3. Нажмите **OK**.

Тенант будет удален.

При удалении тенанта происходит следующее:

- Принадлежащие тенанту сервисы, за исключением агентов, автоматически останавливаются. В разделе **Ресурсы** → **Активные сервисы** эти сервисы будут отображаться с серым статусом.
- Прекращается прием и обработка событий, а уже полученные события удаляются.
- Все ресурсы тенанта удаляются.

- Учетные записи пользователей, у которых есть доступ только к удаленному тенанту, выключаются: активные сессии прерываются, а при попытке повторного входа отображается сообщение об ошибке.

- В разделе **Параметры** → **Доступ** → **Доменная аутентификация** в блоке параметров **Группы администрирования** удаляются фильтры по ролям, созданные для этого тенанта.

Сервисы агентов не останавливаются автоматически. При необходимости вы можете самостоятельно остановить сервисы агентов Windows в разделе **Пуск** → **Сервисы** и остановить сервисы агентов Linux в терминале, где был запущен агент, с помощью комбинации клавиш **`Ctrl`**+**`C`**.

[▷]

https://rutube.ru/video/22238353139675f3127dfa7379ed6c22/

Выбор тенанта

Если вы имеете доступ к нескольким тенантам, в KUMA можно выбрать, данные каких тенантов будут отображаться в веб-интерфейсе KUMA.

Чтобы выбрать тенант для отображения данных:

1. В веб-интерфейсе KUMA нажмите **Выбрано тенантов**.

   Откроется область выбора тенантов.

2. Установите флажки напротив тенантов, данные которых вы хотите видеть в разделах веб-интерфейса KUMA.

3. Требуется выбрать как минимум один тенант. Тенанты можно искать с помощью поля **Поиск**.

4. Закройте область выбора тенантов, нажав **Выбрано тенантов**.

   В разделах веб-интерфейса KUMA отображаются только данные и аналитика, относящаяся к выбранным тенантам.

От выбранных для отображения данных тенантов зависит, какие тенанты можно будет указать при создании ресурсов, сервисов, макетов, шаблонов отчетов, виджетов, инцидентов, активов и других параметров KUMA, где можно выбрать тенант.

Правила принадлежности к тенантам

Правила наследования тенанта

Важно отслеживать, какому тенанту принадлежат создаваемые в KUMA объекты: от этого зависит, кто к ним будет иметь доступ и взаимодействие с какими объектами можно настроить. Правила определения тенанта:

- Тенант объекта (например, сервиса или ресурса) определяется пользователем при его создании.

  После создания объекта выбранный для него тенант невозможно изменить. Ресурсы, однако, можно экспортировать, а затем импортировать в другой тенант.

- Тенант алерта и корреляционного события наследуется от создавшего их коррелятора.

  Название тенанта указывается в поле события `TenantId`.

- Если события разных тенантов, обрабатываемых одним коррелятором, не смешиваются, создаваемые коррелятором корреляционные события наследуют тенант события.

- Тенант инцидента наследуется от алерта.

Примеры мультитенантных взаимодействий

Мультитенантность в KUMA дает возможность централизованно расследовать алерты и инциденты, возникающие в разных тенантах. Ниже приведены сценарии, по которым можно проследить, к каким тенантам принадлежат создаваемые объекты.

> При корреляции событий от разных тенантов в общем потоке **не следует** группировать события по тенанту: то есть не нужно в правилах корреляции в поле **Группирующие поля** указывать поле события `TenantId`. Группировка событий по тенанту необходима, только если нужно не смешивать события от разных тенантов.

> Сервисы, которые должны быть размещены на мощностях главного тенанта, разворачиваются только пользователями с ролью главный администратор.

- **Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на его стороне**

  Условие:

  Коллектор и коррелятор принадлежат тенанту 2 (tenantID=2)

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор тенанта 2.
2. При срабатывании правил корреляции в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища для тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

Инцидент создается пользователем вручную. Тенант инцидента определяется тенантом пользователя. Алерт привязывается к инциденту вручную или автоматически.

- **Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на стороне главного тенанта**

Условие:

- Коллектор развернут на тенанте 2 и принадлежит ему (tenantID=2).
- Коррелятор развернут на стороне главного тенанта.

  Принадлежность коррелятора определяется главным администратором в зависимости того, кто будет расследовать инциденты тенанта 2: сотрудники главного тенанта или тенанта 2. Принадлежность алерта и инцидента зависит от принадлежности коррелятора.

Сценарий 1. Коррелятор принадлежит тенанту 2 (tenantID=2):

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании правил корреляции в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

Результат 1:

- Созданный алерт и привязанные к нему события доступны сотрудникам тенанта 2.

Сценарий 2. Коррелятор принадлежит главному тенанту (tenantID=1):

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании правил корреляции в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
3. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.

4. Создается алерт, привязанный к тенанту с идентификатором tenantID=1.

5. К алерту привязываются события, из-за которых он был создан.

Результат 2:

- Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

- **Централизованная корреляция событий, поступающих от разных тенантов**

  Условие:

  - Развернуто два коллектора: на тенанте 2 и тенанте 3. Оба коллектора отправляют события в один коррелятор.
  - Коррелятор принадлежит главному тенанту. Правило корреляции ожидает события от обоих тенантов.

  Сценарий:

  1. Коллектор тенанта 2 получает и отправляет события в коррелятор главного тенанта.
  2. Коллектор тенанта 3 получает и отправляет события в коррелятор главного тенанта.
  3. При срабатывании правила корреляции в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
  4. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
  5. Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.
  6. К алерту привязываются события, из-за которых он был создан.

  Результат:

  - Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
  - Алерт и привязанные к нему события недоступны сотрудникам тенанта 3.
  - Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

- **Тенант коррелирует свои события, но в главном тенанте дополнительно осуществляется централизованная корреляция событий**

  Условие:

  - Развернуто два коллектора: на главном тенанте и тенанте 2.
  - Развернуто два коррелятора:
    - Коррелятор 1 принадлежит главному тенанту и принимает события с коллектора главного тенанта и коррелятора 2.
    - Коррелятор 2 принадлежит тенанту 2 и принимает события с коллектора тенанта 2.

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор 2.
2. При срабатывании корреляционного правила в корреляторе тенанта 2 создаются корреляционные события с идентификатором тенанта tenantID=2.
   - Коррелятор 2 отправляет корреляционные события в раздел хранилища тенанта 2.
   - Создается алерт 1, привязанный к тенанту с идентификатором tenantID=2.
   - К алерту привязываются события, из-за которых он был создан.
   - Корреляционные события от коррелятора тенанта 2 отправляются в коррелятор 1.
3. Коллектор главного тенанта получает и отправляет события в коррелятор 1.
4. В корреляторе 1 обрабатываются события обоих тенантов. При срабатывании правила корреляции создаются корреляционные события с идентификатором тенанта tenantID=1.
   - Коррелятор 1 отправляет корреляционные события в раздел хранилища главного тенанта.
   - Создается алерт 2, привязанный к тенанту с идентификатором tenantID=1.
   - К алерту привязываются события, из-за которых он был создан.

Результат:

- Алерт 2 и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт 2 и привязанные к нему события доступны сотрудникам главного тенанта.

- **Один коррелятор для двух тенантов**

  Если вы не хотите, чтобы при корреляции события от разных тенантов смешивались, в правилах корреляции в поле **Группирующие поля** следует указывать поле события `TenantId`. В таком случае алерт наследует тенант от коррелятора.

  Условие:

  - Развернуто два коллектора: на тенанте 2 и тенанте 3.
  - Развернут один коррелятор, принадлежащий главному тенанту (tenantID=1). Он принимает события от обоих тенантов, но обрабатывает их независимо друг от друга.

  Сценарий:

  1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
  2. Коллектор тенанта 3 получает и отправляет события в коррелятор.

3. При срабатывании правила корреляции в коррелятоpе создаются корреляционные события с идентификатором тенанта tenantID=1.

   - Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
   - Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.
   - К алерту привязываются события, из-за которых он был создан.

Результат:

- Алерты, созданные на основе событий от тенанта 2 и 3, недоступны сотрудникам тенантов 2 и 3.
- Алерты и привязанные к ним события доступны сотрудникам главного тенанта.

Управление пользователями

Доступ к KUMA может иметь несколько пользователей. Пользователям присваиваются роли пользователей, влияющие на задачи, которые пользователи могут выполнять. У разных тенантов у одного и того же пользователя могут быть разные роли. При этом вы не можете самостоятельно добавлять себе роли, даже если вашей учетной записи присвоена роль Главного администратора – список ролей будет отображаться без возможности изменения.

Вы можете создавать или изменять учетные записи пользователя в разделе веб-интерфейса KUMA **Параметры** → **Пользователи**. Учетные записи пользователей решения также создаются автоматически, если включена интеграция KUMA с Active Directory и пользователь входит в веб-интерфейс KUMA с помощью своей доменной учетной записи в первый раз.

> Всем внутренним пользователям, чьи учетные записи были созданы в веб-интерфейсе KUMA, кроме учетной записи admin, нужно сменить пароль при первом входе в веб-интерфейс KUMA. В дальнейшем этим пользователям требуется регулярно менять пароль в соответствии с корпоративными политиками, но не реже, чем раз в три месяца.

Учетные записи пользователей отображаются в окне **Пользователи** веб-интерфейса KUMA на вкладках **Активные пользователи** и **Неактивные пользователи** в зависимости от статуса учетной записи – *Активная* или *Неактивная*. Пользователей можно искать с помощью поля **Поиск**. Вы можете отсортировать таблицы, нажав на заголовок столбца и выбрав **По возрастанию** или **По убыванию**.

Учетные записи можно создавать, изменять или выключать. При изменении учетных записей (как своей, так и чужих) для них можно сгенерировать API-токен.

Чтобы выключить учетную запись пользователя,

в разделе веб-интерфейса KUMA **Параметры** → **Доступы** → **Пользователи** → **Активные пользователи** установите флажок напротив нужного пользователя и нажмите **Выключить**.

Роли пользователей

Доступ к функциональным возможностям KUMA предоставляется пользователю в соответствии с его ролью. Роль – это набор прав и разрешений на управление решением. В KUMA используются предустановленные роли со сформированными наборами прав доступа, а также пользовательские роли.

Предустановленные роли

При установке KUMA по умолчанию создаются следующие предустановленные роли:

- *Главный администратор* – эта роль предназначена для пользователей, отвечающих за функционирование компонентов KUMA. Например, они устанавливают компоненты KUMA, контролируют работу сервисов в составе этих компонентов создают резервные копии и добавляют пользователей. Эти пользователи имеют полный доступ к KUMA.

- *Администратор тенанта* – эта роль предназначена для пользователей, отвечающих за функционирование компонентов KUMA, принадлежащих определенным тенантам.

- *Аналитик 2-ого уровня* – эта роль предназначена для пользователей, ответственных за настройку системы KUMA для получения и обработки событий определенного тенанта. Они также создают и настраивают правила корреляции.

- *Аналитик 1-ого уровня* – эта роль предназначена для пользователей, ответственных за настройку системы KUMA для получения и обработки событий определенного тенанта. Они также создают и настраивают правила корреляции. Пользователи с этой ролью обладают меньшими правами, чем аналитик второго уровня.

- *Младший аналитик* – эта роль предназначена для пользователей, которые сталкиваются с непосредственными угрозами безопасности определенного тенанта. Пользователь с этой ролью посредством REST API видит ресурсы на Общем тенанте.

- *Работа с НКЦКИ* – эта роль доступна для выбора, если в составе лицензии есть модуль GosSOPKA. Пользователи с этой ролью получают уведомления по умолчанию.

- *Доступ к КИИ* – эта роль доступна для выбора, если в составе лицензии есть модуль GosSOPKA. Пользователи с этой ролью получают уведомления по умолчанию.

- *Чтение общих ресурсов* – эта роль предназначена для работы с Общим тенантом. Пользователи с этой ролью обладают правом на чтение общих ресурсов.

- *Редактирование общих ресурсов* – эта роль предназначена для работы с Общим тенантом. Пользователи с этой ролью обладают правом на изменение параметров общих ресурсов.

> Роли Работа с НКЦКИ и Доступ к КИИ отображаются только при наличии модуля GosSOPKA в лицензии.

Каждой предустановленной роли назначены права на выполнение определенных действий в KUMA.

Пользовательские роли

Если имеющихся предустановленных ролей недостаточно для пользователя, вы можете создать и использовать собственные уникальные наборы прав и разрешений в виде пользовательских ролей.

В разделе **Параметры** → **Доступ** → **Роли** вы можете выполнять следующие действия:

- создавать пользовательские роли, в том числе создавать их с помощью процедуры дублирования на основе существующих ролей (включая предустановленные роли);
- изменять параметры пользовательских ролей;
- просматривать набор прав и полномочий роли, список пользователей с выбранной ролью, а также тенанты пользовательских ролей;
- удалять пользовательские роли.

Права предустановленных ролей

В KUMA права назначаются предустановленным ролям пользователя с учетом раздела решения. Информация о правах пользователей в различных разделах приводится в таблицах ниже.

Права пользователей раздела Отчеты

Раздел Отчеты и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Создавать шаблон отчета	есть	есть	есть	есть	нет	нет	нет	нет	нет
Просматривать и изменять шаблоны и отчеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Формировать отчеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Просматривать сформированные отчеты	есть	есть	есть	есть	есть	нет	нет	нет	нет
Изменять сформированные отчеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Выгружать сформированные отчеты	есть	есть	есть	есть	есть	нет	нет	нет	нет
Удалять шаблоны и сформированные отчеты	есть	есть	есть	есть	нет	нет	нет	нет	нет

Изменять параметры формирования отчетов	есть	есть	есть	есть	нет	нет	нет	нет	нет
Дублировать шаблон отчета	есть	есть	есть	есть	нет	нет	нет	нет	нет
Открывать сформированный отчет по почте	есть	есть	есть	есть	есть	нет	нет	нет	нет

Права пользователей раздела Панель мониторинга

Раздел Панель мониторинга и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать данные на панели мониторинга и менять макеты	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просматривать универсальный макет	есть	есть	есть	есть	есть	нет	нет	есть	есть
Добавлять макеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Изменять и переименовывать макеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Удалять макеты	есть	есть	есть	есть	нет	нет	нет	нет	нет
Включать и выключать режим ТВ	есть	есть	есть	есть	есть	нет	нет	есть	есть

Права пользователей раздела Ресурсы

Раздел Ресурсы → Сервисы и Ресурсы → Сервисы → Активные сервисы и действия в этих разделах	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список активных сервисов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просматривать и удалять партиции в хранилище	есть	нет	нет	нет	нет	нет	нет	нет	нет
Скачивать журналы сервисов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Копировать ID сервиса	есть	есть	есть	есть	есть	нет	нет	есть	есть
Обновить таблицу с активными сервисами	есть	есть	есть	есть	есть	нет	нет	есть	есть
Перейти к событиям	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просматривать содержимое активного листа	есть	есть	есть	есть	нет	нет	нет	нет	нет

Просматривать содержимое контекстной таблицы	есть	есть	есть	есть	нет	нет	нет	нет	нет
Импортировать/экспортировать/очищать/добавлять/редактировать/удалять содержимое активного листа	есть	есть	есть	есть	нет	нет	нет	нет	нет
Импортировать/экспортировать/очищать/добавлять/редактировать/удалять содержимое контекстной таблицы	есть	есть	есть	есть	нет	нет	нет	нет	нет
Создавать набор ресурсов для сервисов	есть	есть	есть	нет	нет	нет	нет	нет	нет
Создавать сервис в разделе Ресурсы → Сервисы → Активные сервисы	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять сервисы	есть	есть	нет	нет	нет	нет	нет	нет	нет
Просматривать сервисы в сером статусе	есть	нет	нет	нет	нет	нет	нет	нет	нет
Перезапускать сервисы	есть	есть	нет	нет	нет	нет	нет	нет	нет
Обновлять параметры сервисов	есть	есть	есть	нет	нет	нет	нет	нет	нет
Сбрасывать сертификаты	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Сбор и анализ данных

Раздел Сбор и анализ данных и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просмотр конфигурации планировщика	есть	есть	есть	нет	нет	нет	есть	нет	нет
Создание планировщика	есть	есть	есть	нет	нет	нет	нет	нет	нет
Привязка хранилищ и корреляторов	есть	есть	есть	нет	нет	нет	нет	нет	нет
Запуск	есть	есть	есть	нет	нет	есть	нет	нет	нет

Права пользователей раздела Конфигурация ресурсов и Конфигурация сервисов

Раздел Ресурсы → Конфигурация ресурсов и Конфигурация сервисов и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список конфигураций ресурсов и сервисов	есть	есть	есть	есть	нет	есть	есть	нет	нет
Создавать конфигурацию сервиса	есть	есть	есть	есть	нет	нет	нет	нет	нет
Создавать конфигурацию ресурса	есть	есть	есть	есть	нет	есть	нет	нет	нет
Дублировать конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	нет	нет	нет
Изменять конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	нет	нет	нет
Удалять конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	нет	нет	нет
Импортировать конфигурацию ресурса/сервиса из файла	есть	есть	есть	есть	нет	есть	нет	нет	нет
Просматривать репозиторий, импортировать ресурсы из репозитория	есть	есть	есть	нет	нет	нет	нет	нет	нет
Экспортировать конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	есть	нет	нет
Экспортировать правила корреляции в MITRE ATT&CK Navigator	есть	есть	есть	есть	нет	нет	нет	нет	нет
Создать и редактировать конфигурацию ресурса в Общем тенанте	есть	нет	нет	нет	нет	есть	есть	нет	нет
Просматривать ресурс в Общем тенанте (в том числе привязать, экспортировать, дублировать)	есть	нет	нет	нет	нет	есть	есть	нет	нет

Права пользователей раздела Список источников событий

Раздел Состояние источников → Список источников событий и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать источники событий	есть	есть	есть	есть	есть	есть	нет	есть	есть
Изменять источники событий	есть	есть	есть	нет	нет	есть	нет	нет	нет
Удалять источники событий	есть	есть	есть	нет	нет	есть	нет	нет	нет

Права пользователей раздела Политики мониторинга

Раздел Состояние источников → Политики мониторинга и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать политики мониторинга	есть	есть	есть	есть	есть	есть	есть	есть	есть
Создавать политики мониторинга	есть	есть	есть	нет	нет	есть	нет	нет	нет
Изменять политики мониторинга	есть	есть	есть	нет	нет	есть	нет	нет	нет
Удалять политики мониторинга	есть	есть	есть	нет	нет	есть	нет	нет	нет

Права пользователей раздела Активы

Раздел Активы и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Активы									
Просматривать список активов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просматривать список категорий	есть	есть	есть	есть	есть	есть	есть	есть	есть
Добавлять/редактировать/удалять категории активов	есть	есть	есть	есть	нет	нет	нет	нет	нет
Добавлять категории активов в Общем тенанте	есть	нет	нет	нет	нет	нет	нет	нет	нет

Привязывать активы к категории активов Общего тенанта	есть	есть	есть	есть	нет	есть	есть	нет	нет
Добавлять активы	есть	есть	есть	есть	нет	нет	нет	нет	нет
Изменять активы	есть	есть	есть	есть	нет	нет	нет	нет	нет
Удалять активы	есть	есть	есть	есть	нет	нет	нет	нет	нет
Импортировать активы из Kaspersky Security Center	есть	есть	есть	есть	нет	нет	нет	нет	нет
Запускать задачи на активах в Kaspersky Security Center	есть	есть	есть	есть	нет	нет	нет	нет	нет
Запускать задачи перемещения актива в группу администрирования Kaspersky Security Center	есть	есть	есть	есть	нет	нет	нет	нет	нет
Запускать задачи на активах в Kaspersky Endpoint Detection and Response	есть	есть	есть	есть	нет	нет	нет	нет	нет
Запуск изменения статуса актива в KICS for Networks	есть	есть	есть	есть	нет	нет	нет	нет	нет
Подтверждать обновления для закрытия уязвимостей активов и соглашаться с лицензионными соглашениями	есть	есть	нет	нет	нет	нет	нет	нет	нет
Редактирование категоризации КИИ в карточке актива	есть	нет	нет	нет	нет	нет	нет	нет	есть
Редактирование пользовательских полей активов (**Параметры** → **Другое** → **Активы**)	есть	есть	есть	есть	нет	нет	нет	нет	нет

Права пользователей раздела Алерты

Раздел Алерты и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список алертов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Изменять уровень важности алертов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Открывать детали алертов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Назначать ответственных пользователей	есть	есть	есть	есть	есть	нет	нет	есть	есть
Закрывать алерты	есть	есть	есть	есть	есть	нет	нет	есть	есть
Добавлять комментарий к алертам	есть	есть	есть	есть	есть	нет	нет	есть	есть
Привязывать событие к алертам	есть	есть	есть	есть	есть	нет	нет	есть	есть

Отвязывать событие от алертов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Изменять и удалять чужие фильтры	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Инциденты

Раздел Инциденты и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список инцидентов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Создавать пустые инциденты	есть	есть	есть	есть	есть	нет	нет	есть	есть
Создавать вручную инциденты из алертов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Изменять уровень важности инцидентов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Открывать детали инцидентов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Назначать исполнителей	есть	есть	есть	есть	есть	нет	нет	есть	есть
Закрывать инциденты	есть	есть	есть	есть	есть	нет	нет	есть	есть
Добавлять комментарии к инцидентам	есть	есть	есть	есть	есть	нет	нет	есть	есть
Привязывать алерты к инцидентам	есть	есть	есть	есть	есть	нет	нет	есть	есть
Отвязывать алерты от инцидентов	есть	есть	есть	есть	есть	нет	нет	есть	есть
Изменять и удалять чужие фильтры	есть	есть	нет	нет	нет	нет	нет	нет	нет
Экспортировать инциденты в НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет
Отправлять файлы в НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет
Скачивать файлы, отправленные в НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет
Экспортировать дополнительные данные инцидентов в НКЦКИ по запросу	есть	нет	нет	нет	нет	нет	нет	есть	нет
Отправка сообщений в НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет
Просмотр сообщений от НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет
Просмотр данных инцидента, экспортированного в НКЦКИ	есть	нет	нет	нет	нет	нет	нет	есть	нет

Права пользователей раздела События

Раздел События и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список событий	есть	есть	есть	есть	есть	нет	нет	есть	есть
Выполнять поиск событий	есть	есть	есть	есть	есть	нет	нет	есть	есть
Открывать детали событий	есть	есть	есть	есть	есть	нет	нет	есть	есть
Открывать статистику	есть	есть	есть	есть	есть	нет	нет	есть	есть
Проводить ретроспективное сканирование	есть	есть	есть	нет	нет	нет	нет	нет	нет
Выгружать события в TSV-файл	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просмотр фильтров (поисковый запрос)	есть	есть	есть	есть	есть	есть	есть	есть	есть
Добавить (сохранить) фильтр	есть	есть	есть	есть	есть	есть	нет	есть	есть
Изменять и удалять чужие папки фильтров	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять свои фильтры	есть	есть	есть	есть	есть	есть	нет	есть	есть
Удалять чужие фильтры	есть	есть	нет	нет	нет	нет	нет	нет	нет
Запускать ktl-обогащение	есть	есть	есть	есть	нет	нет	нет	нет	нет
Запускать задачи на активах Kaspersky Endpoint Detection and Response в деталях событий	есть	есть	есть	есть	нет	нет	нет	нет	нет
Создавать пресеты	есть	есть	есть	есть	есть	есть	нет	есть	есть
Удалять пресеты	есть	есть	есть	есть	есть	есть	нет	есть	есть
Просматривать и использовать пресеты	есть	есть	есть	есть	есть	есть	есть	есть	есть
Выполнять запросы в фоновом режиме	есть	есть	есть	есть	есть	нет	нет	есть	есть

Права пользователей раздела Пользователи и действия

Раздел Параметры → Доступ → Пользователи и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список пользователей	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавлять пользователя	есть	нет	нет	нет	нет	нет	нет	нет	нет

Изменять пользователя	есть	нет	нет	нет	нет	нет	нет	нет	нет
Генерировать токен	есть	есть	есть	есть	есть	есть	есть	есть	есть
Изменять права доступа для токена	есть	есть	есть	есть	есть	есть	есть	есть	есть
Просматривать данные своего профиля	есть	есть	есть	есть	есть	есть	есть	есть	есть
Изменять данные своего профиля	есть	есть	есть	есть	есть	есть	есть	есть	есть

Права пользователей раздела LDAP-сервер

Раздел Параметры→ Интеграции → LDAP-сервер и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры подключения к LDAP	есть	есть	есть	есть	нет	нет	нет	нет	нет
Изменять параметры подключения к LDAP	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	нет	нет	нет	нет	нет
Импортировать активы	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Тенанты

Раздел Параметры → Доступ → Тенанты и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список тенантов	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавлять тенантов	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять тенантов	есть	нет	нет	нет	нет	нет	нет	нет	нет
Экспортировать тенантов	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Доменная аутентификация

Раздел Параметры → Доступ → Доменная аутентификация и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры подключения к Active directory	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры подключения к Active directory	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавлять фильтры по ролям для тенантов	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Общие

Раздел Параметры → Другое → Общее и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры подключения к SMTP	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры подключения к SMTP	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Лицензия

Раздел Параметры → Другое → Лицензия и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список добавленных лицензионных ключей	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавлять лицензионные ключи	есть	нет	нет	нет	нет	нет	нет	нет	нет
Удалять лицензионные ключи	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Kaspersky Security Center

Раздел Параметры → Интеграции → Kaspersky Security Center и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список Kaspersky Security Center-серверов, с которыми выполнена интеграция	есть	есть	есть	есть	нет	нет	нет	нет	нет
Добавлять подключения к Kaspersky Security Center	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять подключения к Kaspersky Security Center	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	нет	нет	нет	нет	нет
Запускать задачи на импорт активов Kaspersky Security Center	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела KICS/KATA

Раздел Параметры → Интеграции → KICS/KATA и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список серверов KICS/KATA, с которыми выполнена интеграция	есть	есть	нет	нет	нет	нет	нет	нет	нет
Добавлять, изменять параметры интеграции с KICS/KATA	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять параметры интеграции с KICS/KATA	есть	есть	нет	нет	нет	нет	нет	нет	нет
Запускать задачи на импорт активов из настройки для KICS/KATA	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Kaspersky Automated Security Awareness Platform

Раздел Параметры → Интеграции → Kaspersky Automated Security Awareness Platform и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры интеграции с ASAP	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с ASAP	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Kaspersky Endpoint Detection and Response

Раздел Параметры → Интеграции → Kaspersky Endpoint Detection and Response и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры подключений	есть	есть	есть	есть	нет	нет	нет	нет	нет
Добавлять, редактировать и отключать подключения при включенном режиме распределенного решения	есть	нет	нет	нет	нет	нет	нет	нет	нет
Включать режим распределенного решения	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавлять подключения при выключенном режиме распределенного решения	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять подключения при выключенном режиме распределенного решения	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Kaspersky CyberTrace

Раздел Параметры→ Интеграции → Kaspersky CyberTrace и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры интеграции с CyberTrace	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с CyberTrace	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела IRP / SOAR

Раздел Параметры → Интеграции → IRP / SOAR и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры интеграции с IRP / SOAR	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с IRP / SOAR	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Kaspersky Threat Lookup

Раздел Параметры→ Интеграции → Kaspersky Threat Lookup и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры интеграции с Threat Lookup	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с Threat Lookup	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Алерты

Раздел Параметры → Другое → Алерты и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры	есть	есть	есть	есть	нет	нет	нет	нет	нет
Изменять параметры	есть	есть	есть	нет	нет	нет	нет	нет	нет
Удалять конфигурацию всего тенанта из параметров	есть	есть	есть	нет	нет	нет	нет	нет	нет

Права пользователей раздела Автоматическая привязка алертов к инцидентам

Раздел Параметры → Другое → Инциденты → Автоматическая привязка алертов к инцидентам и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры	есть	есть	есть	есть	нет	нет	нет	нет	нет
Изменять параметры	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел доступен для учетной записи с ролями Администратор тенанта, Аналитик 2-го уровня и Аналитик 1-го уровня, если роль присвоена в тенанте Main.

Права пользователей раздела Типы инцидентов

Раздел Параметры → Другое → Инциденты → Типы инцидентов и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать справочник категорий	есть	есть	есть	есть	нет	нет	нет	нет	нет
Просматривать карточки категорий	есть	есть	есть	есть	нет	нет	нет	нет	нет
Добавлять категории	есть	есть	нет	нет	нет	нет	нет	нет	нет
Изменять категории	есть	есть	нет	нет	нет	нет	нет	нет	нет
Удалять категории	есть	есть	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела НКЦКИ

Раздел Параметры → Интеграции → НКЦКИ и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры	есть	нет	нет	нет	нет	нет	нет	нет	нет
Изменять параметры	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Аудит активов

Раздел Параметры → Другое → Активы → Аудит активов и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Создавать, клонировать и редактировать параметры	есть	есть	есть	нет	нет	нет	нет	нет	нет
Просматривать параметры	есть	есть	есть	есть	нет	нет	нет	нет	нет
Удалять параметры	есть	есть	есть	нет	нет	нет	нет	нет	нет

Права пользователей раздела Обновление репозитория

Раздел Параметры → Другое → Обновление репозитория и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать параметры	есть	есть	есть	нет	нет	нет	нет	нет	нет
Изменять параметры	есть	нет	нет	нет	нет	нет	нет	нет	нет
Запуск задачи обновление репозитория вручную	есть	есть	есть	нет	нет	нет	нет	нет	нет

Права пользователей раздела Активы

Раздел Параметры → Другое → Активы и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Добавлять, редактировать, удалять поля активов	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Доступ к пространствам

Раздел Параметры → Доступ → Доступ к пространствам и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просмотр списка наборов	есть	нет	нет	нет	нет	нет	нет	нет	нет
Добавление, редактирование, удаление набора пространств	есть	нет	нет	нет	нет	нет	нет	нет	нет
Установка набора пространств по умолчанию	есть	нет	нет	нет	нет	нет	нет	нет	нет
Назначение пользователю набора пространств	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Теги

Раздел Параметры → Другое → Теги и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список тегов	есть	есть	есть	есть	нет	нет	нет	нет	нет

Права пользователей раздела Поля расширенной схемы событий

Раздел Параметры → Другое → Поля расширенной схемы событий и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просмотр таблицы полей расширенной схемы событий	есть	есть	есть	есть	есть	нет	есть	нет	нет
Экспорт полей расширенной схемы событий	есть	есть	есть	есть	есть	нет	есть	нет	нет
Добавление и изменение полей расширенной схемы событий	есть	есть	есть	есть	есть	нет	нет	нет	нет

Импорт полей расширенной схемы событий	есть	есть	есть	есть	есть	нет	нет	нет	нет
Удаление и выключение полей расширенной схемы событий	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Метрики

Раздел Метрики и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Открывать метрики	есть	нет	нет	нет	нет	нет	нет	нет	нет

Права пользователей раздела Диспетчер задач

Раздел Диспетчер задач и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Просматривать список своих задач	есть	есть	есть	есть	есть	нет	нет	есть	есть
Завершать свои задачи	есть	есть	есть	есть	есть	нет	нет	есть	есть
Перезапускать свои задачи	есть	есть	есть	есть	есть	нет	нет	есть	есть
Просматривать список всех задач	есть	есть	есть	есть	есть	нет	нет	есть	есть
Завершать любые задачи	есть	нет	нет	нет	нет	нет	нет	нет	нет
Перезапускать любые задачи	есть	есть	есть	есть	есть	нет	нет	есть	есть
Перезапускать задачи типа Выполнение запроса в фоне	есть	есть	есть	есть	есть	нет	нет	есть	есть
Останавливать задачи типа Выполнение запроса в фоне и запускать выполнение запроса в разделе **События**	есть	есть	есть	есть	есть	нет	нет	есть	есть

Права пользователей разделаCyberTrace

Раздел CyberTrace и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Открывать раздел	есть	нет	нет	нет	нет	нет	нет	нет	нет

Раздел не отображается в веб-интерфейсе, если не настроена интеграция с CyberTrace в разделе **Параметры** → **Интеграции** → **Kaspersky CyberTrace**.

Права пользователей раздела Доступ к данным тенантов

Раздел Доступ к данным тенантов и действия в этом разделе	Главный администратор	Администратор тенанта	Аналитик 2-го уровня	Аналитик 1-го уровня	Младший аналитик	Редактирование общих ресурсов	Чтение общих ресурсов	Работа с НКЦКИ	Доступ к КИИ
Доступ к тенантам	есть	есть	есть	есть	есть	нет	нет	есть	есть
Общий тенант	есть	есть	есть	есть	есть	есть	есть	есть	есть
Главный тенант	есть	есть	есть	есть	есть	нет	нет	есть	есть

Создание пользовательской роли

При создании роли пользователя можно дать этой роли права на создание пользователей и управление ролями. Пользователь с такой ролью может создать для себя другую учетную запись или роль с большим набором прав и разрешений (в том числе полный контроль со стороны администратора). Настоятельно рекомендуем назначать права администратора только доверенным пользователям.

Чтобы создать пользовательскую роль:

1. В разделе **Параметры** → **Доступ** → **Роли** нажмите на кнопку **Добавить**.

   Роль создается включенной, вы можете выключить ее в таблице со списком ролей или в боковой панели с описанием параметров роли.

2. В поле **Название** укажите название пользовательской роли (от 1 до 128 символов в кодировке Unicode).

3. При необходимости добавьте описание роли (максимум 128 символов).

4. В блоке **Список разрешений** установите флажки около нужных функциональных областей и выберите право в каждой области.

   В списке доступных для выбора функциональных областей приводятся отдельные функциональные области и группы функциональных областей. Например, группа **KSC** включает в себя следующие функциональные области: **Общее** (просмотр статусов задач KSC) и **Обновления** (чтение обновлений KSC). Вы можете выбрать группу функциональных областей полностью или указать отдельные функциональные области в составе группы.

Для выбранных функциональных областей нужно указать уровень прав и разрешений. В KUMA доступны следующие права :

- **Управление** (англ. **Manage**) – полные права на работу в функциональной области (чтение, создание, изменение, удаление).
- **Управление только своими** (англ. **Manage created**) – полные права пользователя в функциональной области (чтение и дублирование всех объектов, изменение и удаление своих объектов) для объектов, которые были созданы пользователем.
- **Чтение** (англ. **Read**) – права на чтение объектов.
- **Нет прав** (англ. **No rights**) – отсутствие прав на работу с объектами.

Для каждой функциональной области можно указать только один уровень полномочий.

По умолчанию при создании роли функциональной области присваивается уровень полномочий как у предустановленной роли Младший аналитик.

Вы можете указать права следующим образом:

- Указать права отдельно для каждой выбранной функциональной области, выбрав соответствующие права в столбце **Разрешения** в таблице со списком функциональных областей.
- Выбрать все функциональные области, входящие в группу, и с помощью расположенных над таблицей кнопок с указанием уровня прав определить для них уровень права.
- Выбрать все группы функциональных областей и с помощью расположенных над таблицей кнопок с указанием уровня прав определить для них уровень права.

Если вы назначаете права с помощью расположенных над таблицей кнопок, полномочия присваиваются только тем функциональным областям, для которых они доступны. Например, для функциональной области **События** можно определить полномочия **Нет прав** или **Чтение**. Если вы с помощью расположенной над таблицей кнопки выбираете для выбранных функциональных областей или групп функциональных областей уровень права **Управление**, права изменятся только у тех функциональных областей, для которых доступно **Управление**. Для функциональной области **События**, для которой такое право недоступно, право не изменится.

> Связанные с AI функциональные области отображаются в роли, если по лицензии доступен модуль AI, а связанные с НКЦКИ и КИИ – если по лицензии доступен модуль GosSOPKA.

5. Нажмите на кнопку **Создать**.

   После сохранения роль появится в списке ролей, которые могут быть назначены пользователю в разделе **Параметры** → **Доступ** → **Пользователи**.

> В KUMA 4.2 невозможно создать пользовательскую роль с доступом к тенанту Shared и его ресурсам. Если пользователю нужен доступ к тенанту Shared, ему необходимо назначить роли тенанта Shared. По умолчанию доступ к тенанту Shared есть у Главного администратора и у ролей, у которых есть следующие права : Редактирование общих ресурсов, Чтение общих ресурсов и Доступ к общим панелям мониторинга.

Вы также можете создать пользовательскую роль, скопировав уже существующую роль, в том числе предустановленную.

Чтобы создать роль на основе существующей роли:

1. В разделе **Параметры** → **Доступ** → **Роли** с помощью флажка выберите роль, параметры которой вы хотите скопировать.

2. Нажмите на кнопку **Дублировать**, расположенную над таблицей со списком ролей.

3. В открывшейся боковой панели при необходимости измените название, описание и набор прав роли.

4. Нажмите на кнопку **Создать**.

Функциональные области и доступные им уровни полномочий

Далее в таблице представлены группы функциональных областей KUMA с указанием входящих в них функциональных областей. Для каждой функциональной области приводится описание и перечисляются доступные уровни полномочий, которые определяются для пользовательских ролей.

Группы функциональных областей и входящие в них функциональные области

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Алерты		
Алерты	Работа с алертами	• Управление • Чтение • Нет прав
Группа функциональных областей Инциденты		
Общее	Работа с инцидентами	• Управление • Чтение • Нет прав
Типы	Работа с типами инцидентов	• Управление • Нет прав
НКЦКИ	Экспорт инцидентов в НКЦКИ	• Управление • Нет прав
Группа функциональных областей События		
События	Поиск событий	• Чтение • Нет прав
Группа функциональных областей Реагирование		
Добавление индикатора в список индикаторов компрометации	Добавление индикатора в список запрещенных индикаторов компрометации CyberTrace из карточки события (вручную)	• Управление • Нет прав
KATA	Реагирование средствами KATA	• Управление • Нет прав
KICS	Реагирование средствами KICS	• Управление • Нет прав
KSC	Реагирование средствами KSC	• Управление • Чтение • Нет прав
Active Directory	Реагирование средствами Active Directory	• Управление • Нет прав
KASAP	Перемещение между группами KASAP	• Управление • Чтение • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Активы		
Общее	Работа с активами	• Управление • Чтение • Нет прав
Категоризации активов	Работа с правилами автоматической категоризации активов	• Управление • Чтение • Нет прав
Категоризация активов КИИ	Чтение и изменение параметров при категоризации актива КИИ в карточке актива	• Управление • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Ресурсы		
Коллекторы	Работа с конфигурацией коллектора	• Управление • Управление только своими • Чтение • Нет прав
Корреляторы	Работа с конфигурацией коррелятора	• Управление • Управление только своими • Чтение • Нет прав
Хранилища	Работа с конфигурацией хранилища	• Управление • Управление только своими • Чтение • Нет прав
Агенты	Работа с конфигурацией агента	• Управление • Управление только своими • Чтение • Нет прав
Маршрутизаторы событий	Работа с конфигурацией маршрутизаторов событий	• Управление • Управление только своими • Чтение • Нет прав
Нормализаторы	Работа с конфигурацией нормализатора	• Управление • Управление только своими • Чтение • Нет прав
Коннекторы	Работа с конфигурацией коннектора	• Управление • Управление только своими • Чтение • Нет прав
Точки назначения	Работа с конфигурацией точки назначения	• Управление • Управление только своими • Чтение • Нет прав
Фильтры	Работа с конфигурации фильтра	• Управление • Управление только своими • Чтение • Нет прав
Активный лист	Работа с конфигурацией активного листа	• Управление • Управление только своими • Чтение • Нет прав
Контекстные таблицы	Работа с конфигурацией контекстных таблиц	• Управление • Управление только своими • Чтение • Нет прав
Словари	Работа с конфигурацией словаря	• Управление • Управление только своими • Чтение • Нет прав
Прокси-серверы	Работа с конфигурацией прокси-сервера	• Управление • Управление только своими

Функциональная область	Описание	Возможные значения полномочий
		• Чтение • Нет прав
Секреты	Работа с конфигурацией секрета	• Управление • Управление только своими • Чтение • Нет прав
Шаблоны уведомлений	Работа с конфигурацией шаблона уведомлений	• Управление • Управление только своими • Чтение • Нет прав
Правила агрегации	Работа с конфигурацией агрегационного правила	• Управление • Управление только своими • Чтение • Нет прав
Правила корреляции	Работа с конфигурацией корреляционного правила	• Управление • Управление только своими • Чтение • Нет прав
Правила обогащения	Работа с конфигурацией правила обогащения	• Управление • Управление только своими • Чтение • Нет прав
Правила реагирования	Работа сконфигурацией правила реагирования	• Управление • Управление только своими • Чтение • Нет прав
Правила получения и анализа данных	Работа с правилами получения и анализа данных	• Управление • Управление только своими • Чтение • Нет прав
Правила сегментации	Работа с конфигурацией правил сегментации	• Управление • Управление только своими • Чтение • Нет прав
Панели мониторинга	Работа с панелями мониторинга	• Управление • Управление только своими • Чтение • Нет прав
Шаблоны отчетов	Работа с шаблонами отчетов	• Управление • Управление только своими • Чтение • Чтение только своих • Нет прав
Импорт ресурсов	Импорт любых ресурсов, папок и категорий активов, в том числе с перезаписью существующих	• Управление • Нет прав
Экспорт ресурсов	Экспорт любых ресурсов, папок и категорий активов	• Чтение • Нет прав
Импорт из репозитория	Импорт ресурсов из репозитория	• Управление • Нет прав
Репозиторий	Чтение репозитория ресурсов	• Чтение • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Директории	Работа с директориями	• Управление • Управление только своими • Чтение • Нет прав
Наборы полей	Работа с набором полей, созданным пользователем	• Управление • Управление только своими • Чтение • Нет прав
Панели секретов	Просмотр панели секретов в разделе **Ресурсы**	• Чтение • Нет прав
Группа функциональных областей Создание исключений для корреляционных правил		
Создание исключений	Создание исключений для корреляционных правил	• Управление • Нет прав
Чтение и удаление исключений	Работа с исключениями для корреляционных правил	• Управление • Нет прав
Группа функциональных областей Активные сервисы		
Подгруппа Работа с сервисами		
Коллектор	Работа с сервисом коллектор	• Управление • Чтение • Нет прав
Коррелятор	Работа с сервисом коррелятор	• Управление • Чтение • Нет прав
Активные листы на коррелятоpe	Работа с контентом активного листа и контекстной таблицы на коррелятоpe	• Управление • Чтение • Нет прав
Хранилище	Работа с сервисом хранилище	• Управление • Чтение • Нет прав
Партиции хранилища	Работа с партициями хранилища в активных сервисах	• Управление • Нет прав
Активные запросы к Clickhouse	Работа с активными запросами к ClickHouse	• Управление • Чтение • Нет прав
Агент	Работа с сервисом агент	• Управление • Чтение • Нет прав
Ядро	Работа с сервисом ядро	• Управление • Чтение • Нет прав
Маршрутизатор событий	Работа с сервисом маршрутизатор событий	• Управление • Чтение • Нет прав
Подгруппа Действия		
Обновление конфигурации	Обновление конфигурации активного сервиса	• Управление • Нет прав
Перезапуск	Перезапуск активного сервиса	• Управление • Нет прав
Сброс сертификата	Сброс сертификата активного сервиса	• Управление • Нет прав
Скачивание артефактов активного сервиса	Скачивание артефактов активного сервиса	• Управление • Нет прав
Оставшиеся сервисы из удаленных тенантов	Чтение и удаление оставшихся сервисов из удаленных тенантов	• Управление • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Получение и анализ данных		
Получение и анализ данных	Работа с получением и анализом данных	• Управление • Чтение • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Задачи		
Ретроспективное сканирование	Работа с фоновой задачей ретроспективного сканирования	• Управление • Управление только своими • Чтение • Нет прав
Экспорт событий	Работа с фоновой задачей экспорта событий	• Управление • Управление только своими • Чтение • Нет прав
KTL	Работа с фоновой задачей запроса к KTL	• Управление • Управление только своими • Чтение • Нет прав
KATA	Работа с фоновой задачей запроса к KATA	• Управление • Управление только своими • Чтение • Нет прав
Скачивание активов	Работа с фоновой задачей скачивания активов KSC/KICS	• Управление • Управление только своими • Чтение • Нет прав
Скачивание учетных записей	Работа с фоновой задачей скачивания учетных записей Active Directory	• Управление • Управление только своими • Чтение • Нет прав
Обновление контента KUMA	Работа с фоновой задачей обновления контента KUMA	• Управление • Управление только своими • Чтение • Нет прав
Очистка истории	Работа с фоновой задачей очистки истории ресурсов	• Управление • Управление только своими • Чтение • Нет прав
Обновление файлов политик мониторинга	Работа с фоновой задачей обновления файлов политик мониторинга	• Управление • Управление только своими • Чтение • Нет прав
Экспорт источников событий	Работа с фоновой задачей экспорта источников событий в формате CSV	• Управление • Управление только своими • Чтение • Нет прав
KIRA	Работа с фоновой задачей, просмотр результатов по запросам в KIRA и деобфускации	• Управление • Управление только своими • Чтение • Нет прав
Поиск событий в фоновом режиме	Работа с фоновой задачей запуска поиска событий в фоновом режиме	• Управление • Управление только своими • Чтение • Нет прав
Создание резервной копии партиций	Работа с фоновой задачей создания резервной копии партиций	• Управление • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Восстановление партиций из резервной копии	Работа с фоновой задачей восстановления партиций из резервной копии	• Управление • Нет прав
Импорт резервной копии партиций	Работа с фоновой задачей импорта резервной копии партиций	• Управление • Нет прав
Группа функциональных областей Параметры		
Подгруппа Доступ – Пользователи		
Общее	Работа с пользователями	• Управление • Управление только своими • Чтение • Нет прав
Без доступа к тенантам	Работа с пользователями, не имеющими доступа к тенантам	• Управление • Нет прав
Учетные данные	Работа с созданием токена доступа к REST API, изменение пароля	• Управление • Управление только своими • Нет прав
Подгруппа Доступ – Роли		
Роли	Работа с параметрами пользовательских ролей	• Управление • Чтение • Нет прав
Общее	Работа с назначением ролей пользователям (кроме главного администратора)	• Управление • Чтение • Чтение только своих • Нет прав
Главный администратор	Работа с назначением роли главного администратора	• Управление • Нет прав
Администратор CyberTrace	Работа с ролью администратора в веб-консоли CyberTrace	• Управление • Нет прав
Подгруппа Доступ – Тенанты		
Реестр тенантов	Работа со списком тенантов	• Управление • Чтение
Параметры	Работа со специфичными для KUMA параметрами тенантов (например, лимиты EPS)	• Управление • Нет прав
Подгруппа Доступ – Active Directory		
Настройка параметров доменной аутентификации	Работа с параметрами доступа в систему с помощью ActiveDirectory, FreeIPA	• Управление • Чтение • Нет прав
Учетные записи	Интеграция с LDAP-сервером по тенантам	• Управление • Чтение • Нет прав
Информация об учетной записи	Информация об учетной записи Active Directory	• Чтение • Нет прав
Подгруппа Доступ – Политики безопасности		
Политики безопасности	Работа с конфигурацией политик безопасности	• Управление • Чтение • Нет прав
Подгруппа Доступ – Доступ к пространствам		
Действия с наборами пространств	Работа с наборами пространств событий	• Управление • Нет прав
Назначение наборов пространств пользователям	Назначение и чтение наборов пространств пользователя; назначение наборов пространств по умолчанию	• Управление • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Подгруппа Интеграция		
KTL	Работа с параметрами интеграции с KTL	• Управление • Чтение • Нет прав
CyberTrace	Работа с параметрами интеграции с CyberTrace	• Управление • Чтение • Нет прав
KSC	Управление обновлениями KSC	• Управление • Чтение • Нет прав
KIRA	Работа с параметрами интеграции с KIRA	• Управление • Чтение • Нет прав
KSN	Работа с параметрами интеграции с KSN	• Управление • Чтение • Нет прав
KICS	Работа с параметрами интеграции KICS	• Управление • Чтение • Нет прав
KATA single	Работа с параметрами интеграции с KATA	• Управление • Чтение • Нет прав
KATA multi	Работа с параметрами интеграции с KATA (распределенное решение)	• Управление • Чтение • Нет прав
НКЦКИ	Работа с параметрами НКЦКИ	• Управление • Нет прав
KSN	Работа с параметрами интеграции с KSN	• Управление • Чтение • Нет прав
KASAP	Работа с параметрами интеграции с KASAP	• Управление • Чтение • Нет прав
KIRA	Работа с параметрами интеграции с KIRA	• Управление • Чтение • Нет прав
KSN	Работа с параметрами интеграции с KSN	• Управление • Чтение • Нет прав
Подгруппа Алерты		
Привязка правил сегментации к алертам	Работа с привязкой правил сегментации к алертам	• Управление • Чтение • Нет прав
Привязка шаблонов уведомлений к алертам	Работа с привязкой шаблонов уведомлений к алертам	• Управление • Чтение • Нет прав
Алерты	Работа с параметрами для создания алертов и хранения событий алертов	• Управление • Чтение • Нет прав
Подгруппа Лицензия		
Лицензия	Управление лицензированием	• Управление • Чтение
Подгруппа Инциденты		
Инциденты	Работа с конфигурацией инцидентов	• Управление • Чтение • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Подгруппа Обновление репозитория KUMA		
Обновление репозитория KUMA	Работа с параметрами обновления репозитория KUMA	• Управление • Управление только своими • Чтение • Нет прав
Подгруппа Активы		
Импорт активов	Работа с параметрами импорта активов	• Управление • Чтение • Нет прав
Аудит активов	Работа с параметрами аудита активов	• Управление • Чтение • Нет прав
KSC	Работа с параметрами импорта активов KSC	• Управление • Чтение • Нет прав
Подгруппа Список тегов ресурсов		
Список тегов ресурсов	Работа с тегами ресурсов KUMA	• Чтение • Нет прав
Подгруппа Мониторинг сервисов		
Мониторинг сервисов. Настройка пороговых значений	Работа с пороговыми значениями для алертов каждого типа сервиса	• Управление • Чтение • Нет прав
Подгруппа Поля расширенной схемы событий		
Удаление и изменение полей расширенной схемы событий KUMA	Удаление и изменение статуса `disabled` у полей расширенной схемы событий KUMA	• Управление • Нет прав
Поля расширенной схемы событий KUMA	Работа с полями расширенной схемы событий KUMA (за исключением удаления и изменения статуса `disabled`)	• Управление • Чтение • Нет прав
Подгруппа Игнорирование TTL		
Игнорирование TTL	Настройка игнорирования параметра TTL	• Управление • Нет прав
Подгруппа Обнаружение источников событий		
Обнаружение источников событий	Работа с параметрами обнаружения источников событий	• Управление • Чтение • Нет прав
AI-рейтинг и AI-статус активов		
AI-рейтинг и AI-статус активов	Управление конфигурацией API для параметра `sequence appraiser`	• Управление • Нет прав
Подгруппа Rvision		
Rvision	Работа с параметрами Rvision	• Управление • Нет прав
Подгруппа Доступ к настройкам прав на REST API		
Доступ к настройкам прав на REST API	Работа с настройками списка доступных конечных точек	• Управление • Управление только своими • Нет прав

Функциональная область	Описание	Возможные значения полномочий
Группа функциональных областей Системные операции		
Создание резервной копии	Создание резервной копии KUMA	• Управление • Нет прав
Восстановление	Восстановление из резервной копии KUMA	• Управление • Нет прав
Сертификаты веб-приложения KUMA	Работа с сертификатом веб-приложения KUMA	• Управление • Нет прав
Внутренние сертификаты KUMA	Работа с внутренними сертификатами KUMA	• Управление • Нет прав
Техническое обслуживание	Техническое обслуживание	• Управление • Нет прав
Группа функциональных областей CyberTrace		
CyberTrace	Доступ к веб-консоли CyberTrace	• Чтение • Нет прав
Группа функциональных областей Источники событий		
Источники событий	Работа с источниками событий	• Управление • Чтение • Нет прав
Политики мониторинга	Работа с политиками мониторинга	• Управление • Чтение • Нет прав
Встроенные политики мониторинга	Управление встроенными политиками мониторинга	• Управление • Нет прав
Группа функциональных областей Предустановленные сущности		
Предустановленные сущности	Работа с предустановленными сущностями	• Управление • Чтение • Нет прав
Группа функциональных областей Уведомления		
Получение SMTP-уведомлений	Получение SMTP-уведомлений	• Чтение • Нет прав

Изменение параметров пользовательской роли

Вы не можете изменить параметры предустановленных системных ролей. Вы можете дублировать предустановленные роли и просмотреть карточки ролей (имеющиеся у ролей полномочия и пользователей, которым назначены эти роли).

Чтобы изменить параметры пользовательской роли:

1. В разделе **Параметры** → **Доступ** → **Роли** нажмите на название пользовательской роли в таблице со списком ролей.

2. В открывшейся боковой панели с помощью переключателя при необходимости измените состояние роли – активная или неактивная.

Когда вы изменяете состояние роли и делаете ее неактивной, роль становится недоступной для назначения пользователям. Если эта роль была назначена пользователю, ему становятся недоступны полномочия роли. Если пользователю была назначена только эта роль, его сессия прерывается. В разделе **Параметры** → **Доступ** → **Пользователи** такой пользователь более не отображается в блоке активных пользователей, а указывается в списке неактивных пользователей. В карточке такого пользователя отображается предупреждение о необходимости назначить хотя бы одну роль пользователю или удалить пользователя.

Когда вы изменяете состояние роли и делаете ее активной, роль добавляется в список ролей, которые могут быть назначены пользователю.

После перевода роли в активное состояние пользователь, которому эта роль назначена, автоматически не становится активным пользователем в разделе **Параметры** → **Доступ** → **Пользователи**. Вам нужно активировать пользователя.

По умолчанию пользовательская роль создается в активном состоянии.

3. При необходимости измените название, описание и набор полномочий пользовательской роли. С помощью фильтра **Показать функциональные области** вы можете выбрать интересующий вас уровень полномочий. KUMA отобразит только те функциональные области, для которых установлены выбранные вами полномочия.

4. Нажмите на кнопку **Сохранить**.

Просмотр параметров роли

Чтобы посмотреть набор прав роли,

в разделе **Параметры** → **Доступ** → **Роли** нажмите на название роли в столбце **Название** в таблице со списком ролей пользователей.

В открывшейся боковой панели справа в блоке **Список разрешений** отображается набор прав по функциональным областям роли.

Чтобы посмотреть список пользователей с выбранной ролью и тенанты, в которых роль будет назначена пользователям:

1. Перейдите в раздел **Параметры** → **Доступ** → **Роли**.

2. Выполните одно из следующих действий:

   - Нажмите на число, указанное для роли в столбце **Пользователи** в таблице со списком ролей.

   - Нажмите на название роли в столбце **Название** и в открывшемся окне перейдите на вкладку **Пользователи и группы**.

   В открывшемся окне отображаются пользователи, которым назначена роль. Вы можете посмотреть активных и неактивных пользователей с указанием имени пользователя, логина, адреса электронной почты. Для каждого пользователя также указывается количество назначенных ему ролей и тенант, к которому относится пользователь. Если вы перейдете по ссылке с числом, указанным для роли в столбце **Пользователи,** вы можете изменить учетную запись пользователя.

Удаление пользовательской роли

Чтобы удалить пользовательские роль:

1. В разделе **Параметры** → **Доступ** → **Роли** с помощью флажков выберите роль или несколько ролей, которые вы хотите удалить.

2. Нажмите на кнопку **Удалить**, расположенную над таблицей со списком ролей.

   Кнопка **Удалить** активируется только при выборе пользовательских ролей для удаления. Предустановленные роли невозможно удалить.

3. Для подтверждения удаления выполните одно из следующих действий:

   - Если роль была назначена пользователю, введите код подтверждения и нажмите **OK**.

   - Если роль не была назначена пользователю, нажмите **OK**.

   KUMA удаляет роль из списка ролей, а пользователям, которым эта роль была назначена, становятся недоступны права роли. Если роль удаляется во время активного сеанса пользователей, которым была назначена только эта роль, сеанс прерывается. Таким пользователям необходимо назначить другие роли или нужно удалить таких пользователей.

Настройка политики безопасности при входе в веб-интерфейс

Чтобы снизить риск несанкционированного доступа к веб-интерфейсу KUMA, вы можете настроить правила входа в веб-интерфейс KUMA для пользователей. Например, настроенная политика безопасности помогает предотвратить вход злоумышленника в веб-интерфейс KUMA с помощью перебора пароля.

Политика безопасности действует только на учетные записи пользователей, созданные в KUMA, и не действует на доменные учетные записи, импортированные в KUMA при интеграции с контроллерами доменов. При этом политика безопасности ограниченно действует на учетную запись admin, которая используется для первого входа в веб-интерфейс KUMA. Из всех параметров политики безопасности к этой учетной записи применяется только параметр принудительной повторной аутентификации при бездействии пользователя.

Политика безопасности применяется ко всем тенантам и не может быть настроена для каждого тенанта в отдельности.

При обновлении с предыдущей версии KUMA требования к паролям применяются только к новым паролям. Существующие пароли попадают под действие только параметра **Время жизни пароля (дни)**, остальные требования к таким паролям не применяются. Пользователям, чьи пароли не менялись дольше 90 дней, KUMA после обновления предложит сменить пароль.

Параметры политики безопасности может менять только пользователь с ролью Главный администратор.

Чтобы настроить политику безопасности при входе в веб-интерфейс KUMA:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Доступ** → **Настройки политики безопасности**.

2. Укажите следующие параметры безопасности:

   - **Максимальное количество неудачных попыток аутентификации** – при превышении указанного значения учетная запись пользователя блокируется на время, указанное в параметре **Длительность блокировки учетной записи после неудачных попыток аутентификации (мин)**. Укажите число от 0 до 10. Значение 0 выставлено по умолчанию и означает, что этот параметр выключен.

   - **Максимальное количество попыток аутентификации в секунду на Ядро** – этот параметр помогает предотвратить вход в веб-интерфейс KUMA с помощью автоматического перебора пароля. Укажите число от 1 до 8. Значение по умолчанию – 3. Если KUMA фиксирует превышение заданного значения, дальнейшие попытки аутентификации блокируются.

     Обратите внимание, что параметр указывается в расчете на одно Ядро KUMA. Если в вашем экземпляре KUMA развернуто больше одного Ядра KUMA, фактическое разрешенное количество попыток аутентификации в секунду будет равно указанному вами значению, умноженному на количество Ядер KUMA.

   - **Длительность блокировки учетной записи после неудачных попыток аутентификации (мин)** – период, на который учетная запись блокируется при превышении значения параметра **Максимальное количество неудачных попыток аутентификации**. Укажите число от 0 до 1440. Значение по умолчанию – 15. Значение 0 означает, что статус учетной записи сменится на *Неактивная*. Пользователь с таким статусом не может войти в веб-интерфейс KUMA. Главный администратор может изменить статус учетной записи позже. Если Главный администратор меняет статус учетной записи на *Активная*, учетная запись будет разблокирована, счетчик неудачных попыток входа будет сброшен на 0.

   - **Запретить пользователям входить в систему после истечения срока действия пароля** – этот параметр позволяет вам выбрать поведение решения после истечения срока, указанного в параметре **Время жизни пароля (дни)**.

     Если этот параметр включен, попытка пользователя войти в веб-интерфейс KUMA будет заблокирована. Статус учетной записи пользователя сменится на *Неактивная*. Пользователь с таким статусом не может войти в веб-интерфейс KUMA. Главный администратор может изменить статус учетной записи позже. Попытка входа пользователя будет заблокирована, даже если у пользователя включена настройка **Пользователь должен сменить пароль при следующем входе в систему**.

     Если этот параметр выключен, пользователь с истекшим паролем сможет войти в веб-интерфейс KUMA. После этого KUMA автоматически предложит пользователю сменить пароль.

   - **Повторная аутентификация требуется после того, как пользователь неактивен в течение (мин)** – если во время сеанса в веб-интерфейсе KUMA не будет зафиксировано движение мыши или нажатия клавиш со стороны пользователя в течение указанного вами периода, KUMA потребует повторную аутентификацию пользователя. Укажите число от 1 до 1440. Значение по умолчанию – 15.

3. Укажите следующие параметры паролей пользователей:

   - **Время жизни пароля (дни)** – после истечения времени жизни пароля KUMA либо блокирует, либо не блокирует учетную запись пользователя в зависимости от параметра **Запретить пользователям входить в систему после истечения срока действия пароля**. Укажите число от 1 до 365. Значение по умолчанию – 90.

   - **Минимальная длина пароля (символов)** – укажите число от 16 до 128. Значение по умолчанию – 16.

- **Время уведомления пользователя до истечения срока действия пароля (дни)** – за указанное количество дней до истечения срока действия пароля пользователю в веб-интерфейсе KUMA каждый день будет отображаться уведомление с предложением сменить пароль. Укажите число от 1 до 14. Значение по умолчанию – 14.

- **Обязательные категории символов для пароля** – в этом параметре вы можете задать требования к паролям, как введенным вручную, так и сгенерированным автоматически:

  - Пароль должен содержать буквы латинского алфавита в нижнем регистре, в верхнем регистре, цифры, а также хотя бы один из указанных вами специальных символов.

  - **Игнорировать повторяющиеся символы в пароле** – если этот переключатель включен, в паролях разрешены два или более одинаковых символа подряд.

4. Нажмите **Сохранить**.

Политика безопасности настроена.

Создание учетной записи пользователя

Чтобы создать учетную запись пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Доступ** → **Пользователи**.

2. Нажмите на кнопку **Создать** и задайте параметры, как описано ниже.

   - **Активная** – включите этот переключатель, чтобы сделать учетную запись пользователя активной. По умолчанию переключатель включен.

     В веб-интерфейс KUMA могут входить только пользователи со статусом учетных записей *Активная*. Статус учетной записи также может смениться на *Неактивная* автоматически, например, если превышено максимально допустимое количество попыток входа в веб-интерфейс решения и при этом в параметре **Длительность блокировки учетной записи после неудачных попыток аутентификации** указано значение 0.

   - **Имя** – введите имя пользователя. Длина должна быть от 1 до 128 символов в кодировке Unicode.

   - **Логин** – введите уникальный логин учетной записи пользователя. Длина должна быть от 3 до 64 символов, допускается использование только символов a–z, A–Z, 0–9, . \ - _.

   - **Адрес электронной почты** – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

   - **Часовой пояс** – выберите часовой пояс, в котором будут отображаться временные метки при работе в KUMA. Список формируется на основе параметров операционной системы пользователя и учитывает переход на летнее и зимнее время. По умолчанию используется часовой пояс браузера пользователя.

   - **Использовать формат ISO 8601** – установите этот флажок, чтобы временные метки отображались 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 системе KUMA. Настроенный формат сохраняется в параметрах Ядра KUMA.

   - **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от KUMA.

- **Уведомлять об алертах в веб-интерфейсе** – установите этот флажок, чтобы в веб-интерфейсе KUMA отображались уведомления об алертах. Снимите флажок, если хотите выключить отображение уведомлений. По умолчанию флажок установлен.

- **Отображать непечатаемые символы** – установите этот флажок, 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 выключать с помощью клавиш **`Ctrl`**/**`Command`**+**`*`**.

  Пробелы и знаки табуляции отображаются во всех полях ввода, кроме поля **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.

- **Новый пароль** – введите новый пароль. Вы можете либо задать пароль вручную, либо нажать на кнопку **Сгенерировать пароль**. Пароль должен соответствовать следующим требованиям:

  - длина соответствует политике безопасности;
  - как минимум один символ в нижнем регистре;
  - как минимум один символ в верхнем регистре;
  - как минимум одна цифра;
  - как минимум один специальный символ из списка специальных символов в политике безопасности;
  - не более двух одинаковых символов подряд;
  - пароль не содержит логин.

Пользователю нужно сменить пароль при первом входе в веб-интерфейс KUMA и в дальнейшем менять пароль не реже, чем раз в три месяца. Главный администратор может настроить оба этих параметра в политике безопасности.

- **Подтверждение пароля** – повторите пароль.

- **Пользователь должен сменить пароль при следующем входе в систему** – установите этот флажок, чтобы при следующей попытке входа в веб-интерфейс KUMA пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс KUMA с новым паролем. По умолчанию этот флажок установлен.

  Этот параметр доступен только для учетных записей в статусе *Активная*.

  Например, вы можете использовать этот параметр при создании пользователя. Пользователю можно назначить временный пароль и установить этот флажок. После входа с временным паролем KUMA предложит пользователю сменить пароль.

  Вы также можете назначить пользователям сброс пароля в разделе **Параметры** → **Доступ** → **Пользователи**, выбрав пользователей из списка и нажав на кнопку **Сбросить пароль при следующем входе в систему**.

- В блоке параметров **Доступ** с помощью кнопок **Добавить роль** укажите, какие роли и в каких тенантах будут назначены учетной записи пользователя. Пользователю можно назначить разные роли в разных тенантах, в одном тенанте можно назначить несколько ролей.

- 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.

- **Неограниченный срок действия пароля** – установите этот флажок, чтобы на учетную запись пользователя не действовал параметр **Время жизни пароля**.

  Рекомендуем включать этот параметр для служебной учетной записи, ограничить такой учетной записи права и установить пароль максимальной сложности. Обычно учетная запись с неограниченным временем жизни пароля используется для мониторинга. При переносе пользователей вы можете включить этот параметр вручную для тех служебных учетных записей, которые ранее использовались для отображения панели мониторинга.

3. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**.

   При нажатии на эту кнопку отображается окно создания токена.

4. При необходимости настройте доступные пользователю операции через REST API с помощью кнопки **Права доступа через API**.

5. Нажмите **Сохранить**.

Учетная запись пользователя создана и отображается в таблице **Пользователи**.

Изменение учетной записи пользователя

Чтобы изменить учетную запись пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Доступ** → **Пользователи**.

2. Выберите нужного пользователя и в открывшейся в правой части области деталей пользователя измените нужные параметры.

   Если вы хотите изменить свою учетную запись, вы также можете в левом нижнем углу окна нажать на имя учетной записи пользователя и в открывшемся меню нажать на кнопку **Профиль**.

   - **Активная** – включите этот переключатель, чтобы сделать учетную запись пользователя активной. По умолчанию переключатель включен.

     > Пользователь не может деактивировать свою собственную учетную запись.

     В веб-интерфейс KUMA могут входить только пользователи со статусом учетных записей *Активная*. Статус учетной записи также может смениться на *Неактивная* автоматически, например, если превышено максимально допустимое количество попыток входа в веб-интерфейс решения и при этом в параметре **Длительность блокировки учетной записи после неудачных попыток аутентификации** указано значение 0.

   - **Имя** – измените имя пользователя. Длина должна быть от 1 до 128 символов в кодировке Unicode.

   - **Логин** – введите уникальный логин учетной записи пользователя. Длина должна быть от 3 до 64 символов (допускается использование только символов a–z, A–Z, 0–9, . \ - _).

- **Адрес электронной почты** – измените адрес электронной почты пользователя. Адрес электронной почты должен быть действительным и уникальным.

- **Часовой пояс** – выберите часовой пояс, в котором будут отображаться временные метки при работе в KUMA. Список формируется на основе параметров операционной системы пользователя и учитывает переход на летнее и зимнее время. По умолчанию используется часовой пояс браузера пользователя.

- **Использовать формат ISO 8601** – установите этот флажок, чтобы временные метки отображались 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 системе KUMA. Настроенный формат сохраняется в параметрах Ядра KUMA.

- **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от KUMA.

- **Уведомлять об алертах в веб-интерфейсе** – установите этот флажок, чтобы в веб-интерфейсе KUMA отображались уведомления об алертах. Снимите флажок, если хотите выключить отображение уведомлений. По умолчанию флажок установлен.

- **Отображать непечатаемые символы** – установите этот флажок, 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 выключать, нажимая клавиши **`Ctrl/Command+*`**.

  Пробелы и знаки табуляции отображаются во всех полях ввода, кроме поля **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 блоке параметров **Доступ** с помощью кнопок **Добавить роль** укажите, какие роли и в каких тенантах будет исполнять пользователь. Пользователю можно назначить разные роли в разных тенантах, в одном тенанте можно назначить несколько ролей. Для доменного пользователя в карточке пользователя заблокирована возможность изменения основных ролей (Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик) и доступно добавление и удаление дополнительных ролей (Доступ к КИИ, Работа с НКЦКИ, Чтение общих ресурсов), включая управление привязкой дополнительных ролей к тенантам.

- 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.

3. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **OK**.

   - **Старый пароль** – введите действующий пароль учетной записи. Поле доступно, если вы меняете пароль своей учетной записи.

   - **Новый пароль** – введите новый пароль. Вы можете либо задать пароль вручную, либо нажать на кнопку **Сгенерировать пароль**. Пароль должен соответствовать следующим требованиям:

     - длина соответствует политике безопасности;

     - как минимум один символ в нижнем регистре;

- как минимум один символ в верхнем регистре;
- как минимум одна цифра;
- как минимум один специальный символ из списка специальных символов в политике безопасности;
- не более двух одинаковых символов подряд;
- пароль отличается от трех последних паролей этой учетной записи;
- пароль не содержит логин.

- **Подтверждение пароля** – повторите пароль.
- **Пользователь должен сменить пароль при следующем входе в систему** – установите этот флажок, чтобы при следующей попытке входа в веб-интерфейс KUMA пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс KUMA с новым паролем. По умолчанию флажок установлен.

  Этот параметр доступен только для учетных записей в статусе *Активная*.

4. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно создания токена.
5. При необходимости настройте доступные пользователю операции через REST API с помощью кнопки **Права доступа через API**.
6. **Неограниченный срок действия пароля** – установите этот флажок, чтобы на учетную запись не действовал параметр **Время жизни пароля**.

   Рекомендуем включать этот параметр для служебной учетной записи, ограничить такой учетной записи права и установить пароль максимальной сложности. Обычно учетная запись с неограниченным временем жизни пароля используется для мониторинга. При миграции пользователей вы можете включить этот параметр вручную для тех служебных учетных записей, которые ранее использовались для отображения панели мониторинга.
7. Нажмите **Сохранить**.

Учетная запись пользователя изменена.

Особенности изменения набора пространств, назначенных пользователю

Пользователю назначаются один или несколько наборов пространств, информация о которых сохраняется в параметрах учетной записи пользователя. Пространства в составе набора пространств можно просмотреть, если в профиле пользователя навести курсор мыши на набор пространств. При необходимости состав набора пространств можно изменить в разделе **Параметры** → **Доступ** → **Доступ к пространствам**.

Если пространство удаляется из хранилища, это пространство продолжает отображаться в составе набора пространств с обозначением `удалено+UUID`. При этом показываются только первые 8 символов универсального уникального идентификатора (UUID) пространства. Удаленное пространство перестает отображаться в составе набора пространств после сохранения изменений в этом наборе пространств.

> Пространство полностью удаляется из набора пространств, если в этом пространстве нет событий. Если события в удаляемом пространстве зафиксированы, KUMA будет отображать это пространство как `удалено+UUID` даже после сохранения изменений в наборе пространств.

Сервисы KUMA

Сервисы – это основные компоненты KUMA, с помощью которых система осуществляет работу с событиями: сервисы 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 сервиса создается внутри веб-интерфейса 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 агента или хранилища могут быть установлены сразу на нескольких устройствах.

  > В серверной части сервисы KUMA располагаются в директории `/opt/kaspersky/kuma`.

  При установке KUMA в отказоустойчивом варианте в кластере устанавливается только Ядро KUMA. Коллекторы, корреляторы и хранилища размещаются на хостах вне кластера Kubernetes.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Типы сервисов:

- Хранилища – используются для хранения событий.
- Корреляторы – используются для анализа событий и поиска заданных закономерностей.
- Коллекторы – используются для получения события и конвертации их в формат KUMA.
- Агенты – используются для получения событий на удаленных устройствах и пересылки их в коллекторы KUMA.
- Маршрутизаторы событий – используются для приема потоков событий от коллекторов и корреляторов и дальнейшего распределения событий по заданным точкам назначения в соответствии с настроенными фильтрами.

В веб-интерфейсе KUMA сервисы отображаются в разделе **Ресурсы** → **Активные сервисы** в виде таблицы. Таблицу сервисов можно обновить с помощью кнопки **Обновить** и сортировать по столбцам, нажимая на активные заголовки. Также вы можете настроить отображение столбцов в таблице с помощью раскрывающегося списка, который вы можете вызвать, нажав на кнопку в виде шестеренки в верхнем правом углу. В раскрывающемся списке установите флажок рядом с названиями тех столбцов, которые вы хотите отображать в таблице. Вы можете оставить для отображения только один любой столбец из списка.

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 и доступен с сервера Ядра.
  - Красный – сервис не работает или не доступен с сервера Ядра.
  - Желтый – этот статус применяется ко всем сервисам, кроме агента. Желтый статус означает, что сервис работает, но в журнале сервиса есть ошибки или для сервиса есть алерты от Victoria Metrics. Сообщение об ошибке можно просмотреть, если навести курсор мыши на статус сервиса в разделе **Активные сервисы**.
  - 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 Victoria Metrics, статус сервиса будет желтым.
  - Серый – если в удаленном тенанте был работающий сервис, который продолжает работать, на странице Активные сервисы он будет отображаться с серым статусом. 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 Главному тенанту.
- **Тип** – вид сервиса: **агент**, **коллектор**, **коррелятор**, **хранилище**, **маршрутизатор событий**.
- **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** – время работы сервиса.
- **Создан** – дата и время создания сервиса.
- **UUID** – уникальный идентификатор сервиса.

  По умолчанию этот столбец не отображается в таблице. Вы можете добавить его в таблицу, нажав на значок шестеренки ⚙ в верхней правой части таблицы сервисов и установив флажок напротив названия столбца **UUID** в раскрывающемся списке.

В таблице предусмотрена сортировка данных по возрастанию и убыванию, а также по параметру **Статус** и по типу сервиса в столбце **Тип**. Вы можете отсортировать активные сервисы, вызвав контекстное меню правой кнопкой мыши и выбрав один или несколько статусов и тип.

С помощью кнопок в верхней части окна **Сервисы** можно выполнить следующие групповые действия:

- **Добавить сервис**

  Вы можете создавать новые сервисы на основе существующих наборов ресурсов для сервисов. Мы не рекомендуем создавать сервисы вне основного тенанта без предварительного внимательного планирования межтенантных взаимодействий различных сервисов и пользователей.

- **Обновить**

  Вы можете обновить список активных сервисов.

- **Обновить параметры**

  Кнопка **Обновить параметры** не будет доступна, если среди сервисов, выбранных для групповых действий, есть сервис Ядра KUMA или какой-либо из выбранных сервисов находится в сером статусе. Чтобы кнопка **Обновить параметры** стала доступна для групповых действий, снимите флажок с сервиса Ядра KUMA и сервисов в сером статусе.

- **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.

- Копировать идентификатор сервиса

  Идентификатор понадобится вам для установки, перезапуска, остановки или удаления сервиса.

- Перейти к событиям

- Смотреть активные листы

- Смотреть контекстные таблицы

- Смотреть разделы

Чтобы изменить сервис, выберите сервис 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. При необходимости 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 разделе веб-интерфейса KUMA **Ресурсы** → **Активные сервисы**.

Изменение названия сервиса

При необходимости вы можете изменить имя и параметры созданных сервисов.

Чтобы изменить название сервиса:

1. В веб-интерфейсе откройте раздел **Ресурсы** → **Активные сервисы**.
2. Нажмите на ссылку с названием сервиса в столбце **Сервис**.
3. В открывшемся окне укажите новое название сервиса и при необходимости измените параметры. Название должно быть уникальным в рамках одного тенанта и содержать от 1 до 128 символов в кодировке Unicode.

   Для сервисов Ядро KUMA и сервиса Метрики доступно только изменение названия.
4. Нажмите на кнопку **Сохранить**.

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса – расположенных внутри KUMA и установленных в сетевой инфраструктуре – в единый комплекс. Идентификатор присваивается сервису при его создании в KUMA, а затем используется при установке сервиса на сервер.

Чтобы получить идентификатор сервиса:

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. В контекстном меню названия сервиса, идентификатор которого вы хотите получить, выберите **Копировать идентификатор**.

Идентификатор сервиса помещен в буфер. Его можно использовать, например, для установки сервиса на сервере.

Остановка, запуск и проверка статуса сервиса

В ходе работы с KUMA 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 представлены команды, которые могут быть полезны во время работы с KUMA.

Команды остановки, запуска и проверки статуса сервиса

Сервис	Остановить сервис	Запустить сервис	Провери
Ядро	`sudo systemctl stop kuma-core-` `< идентификатор сервиса >.service`	`sudo systemctl start kuma-core-` `< идентификатор сервиса >.service`	`sudo systemctl s` `< идентификатор`

Сервисы с идентификатором:
• коллектор
• коррелятор
• хранилище
• метрики
	`sudo systemctl stop kuma-`
	`<collector/correlator/storage/metrics>-`
	`< идентификатор сервиса >.service`
		`sudo systemctl start kuma-`
		`<collector/correlator/storage/metrics>-`
		`< идентификатор сервиса >.service`
			`sudo systemctl s`
			`<collector/corre`
			`< идентификатор`

Агенты под управлением ОС Windows	Чтобы остановить сервис агента:
	1. Скопируйте в веб-интерфейсе KUMA идентификатор агента.
	2. Подключитесь к хосту, на котором необходимо выполнить запуск службы агента KUMA.
	3. Запустите интерпретатор команд PowerShell от имени учетной записи с правами администратора.
	4. Выполните в PowerShell команду:
	`Stop-Service -Name "WindowsAgent-`
	`< идентификатор агента >"`
		Чтобы запустить сервис агента:
		1. Скопируйте в веб-интерфейсе KUMA идентификатор агента.
		2. Подключитесь к хосту, на котором необходимо выполнить запуск службы агента KUMA.
		3. Запустите интерпретатор команд PowerShell от имени учетной записи с правами администратора.
		4. Выполните в PowerShell команду:
		`Start-Service -Name "WindowsAgent-`
		`< идентификатор агента >"`
			Чтобы просмотрет
			1. В ОС Windows пе Services и в списке двойным щелчком н
			2. В открывшемся о просмотрите стату status.

Перезапуск сервиса

Чтобы перезапустить сервис:

1. В веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом и выберите один из следующих вариантов:
   - **Обновить параметры** – обновить конфигурацию работающего сервиса, не останавливая его. Например, так можно изменить параметры сопоставления полей или параметры точки назначения.
   - **Перезапустить** – остановить сервис и запустить его снова. Этот вариант используется для изменения таких параметров, как порт или тип коннектора.

Особенности перезапуска агентов KUMA:

- Агент KUMA для Windows может быть перезагружен, как описано выше, только если он запущен на удаленном компьютере. Если сервис на удаленном компьютере неактивен, при попытке перезагрузки из KUMA отобразится сообщение об ошибке. В этом случае следует перезапустить сервис Агент KUMA для Windows на удаленном компьютере с Windows. Чтобы узнать, как перезапустить сервисы Windows, обратитесь к документации, относящейся к версии операционной системы вашего удаленного компьютера с Windows.

- Агент KUMA для Linux при использовании этой опции останавливается. Для запуска агента необходимо выполнить команду, с помощью которой он был запущен.

- **Сбросить сертификат** – удалить сертификаты, используемые сервисом для внутренней связи. Этот вариант недопустимо использовать для обновления сертификата Ядра. Чтобы обновить сертификаты Ядра KUMA, их следует перевыпустить.

  Особенности удаления сертификатов для агентов Windows:

  - Если агент находится в зеленом статусе и вы выбрали **Сбросить сертификат**, KUMA удаляет действующий сертификат и создает новый, агент продолжает работу с новым сертификатом.

  - Если агент находится в красном статусе и вы выбрали **Сбросить сертификат**, KUMA отображает ошибку о том, что агент не запущен. В папке установки агента `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<ID агента>\certificates` следует вручную 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:

  1. Независимо от статуса агента необходимо выбрать вариант **Сбросить сертификат** через веб-интерфейс, чтобы удалить сертификат в базах.

  2. В папке установки агента `/opt/kaspersky/agent/<ID агента>/certificates` следует вручную удалить файлы `internal.cert` и `internal.key`.

  3. Поскольку вариант **Сбросить сертификат** останавливает агент, для продолжения работы следует вручную запустить агент. При запуске агента новый сертификат будет создан автоматически.

Удаление сервиса

Перед удалением сервиса получите его идентификатор. Идентификатор потребуется, чтобы удалить сервис с сервера.

Чтобы удалить сервис в веб-интерфейсе KUMA:

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.

2. В контекстном меню названия сервиса выберите **Удалить**.

3. В открывшемся окне подтверждения нажмите **OK**.

Сервис удален из KUMA.

Чтобы удалить сервис с сервера, выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage/eventRouter/metrics> --core https://<FQDN сервера Ядра KUMA>:<порт, используемый ядром KUMA для внутренних коммуникаций (по умолчанию 7210)> --id <идентификатор сервиса> --uninstall
```

Например:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id 29fd6760-a870-42d2-8ebe-eb911ac90305 --uninstall
```

Сервис бдует удален с сервера.

Просмотр таблицы разделов хранилища

Создав и установив сервис хранилища, вы можете просмотреть его разделы в таблице **Разделы**.

*Чтобы открыть таблицу **Разделы**:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть разделы**.

   Откроется таблица **Разделы**.

Таблица содержит следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные.
- **Создан** – дата создания раздела.
- **Пространство** – название раздела.
- **Размер** – размер раздела.
- **События** – количество хранимых событий.
- **Начало холодного хранения** – 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 отфильтровать разделы в таблице по тенантам и пространствам. Для этого нужно нажать на заголовок необходимого столбца и в раскрывающемся списке выбрать фильтры. Набор фильтров, доступный в раскрывающемся списке, зависит от выбранного столбца.

Вы можете удалять разделы.

Чтобы удалить раздел:

1. Откройте таблицу **Разделы** (см. выше).
2. Установите флажок рядом с нужным хранилищем и нажмите **Удалить**.

   Откроется окно подтверждения.
3. Нажмите **OK**.

Раздел будет удален. Разделы для событий аудита удалить невозможно.

Просмотр таблицы активных запросов

Под учетной записью с правами Главного администратора вы можете просмотреть запросы других пользователей и ресурсов KUMA, которые выполняются в этот момент.

Чтобы просмотреть таблицу активных запросов:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажки рядом с нужными хранилищами.
3. В панели инструментов или в меню (⋮) нажмите **Активные запросы**.

   Откроется таблица **Активные запросы в ClickHouse**. Если вы выбрали несколько 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 KUMA. 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 KUMA 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 обновить данные принудительно 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 запросом, который вы хотите отменить, и нажмите **Отменить запрос**. Вы можете выбрать один или несколько запросов.

   Откроется окно подтверждения.
3. При необходимости в поле **Укажите причину** укажите причину отмены выполнения запроса.
4. Нажмите **OK**.

Запрос будет отменен и удален из таблицы. Автоматически создастся событие аудита.

Поиск связанных событий

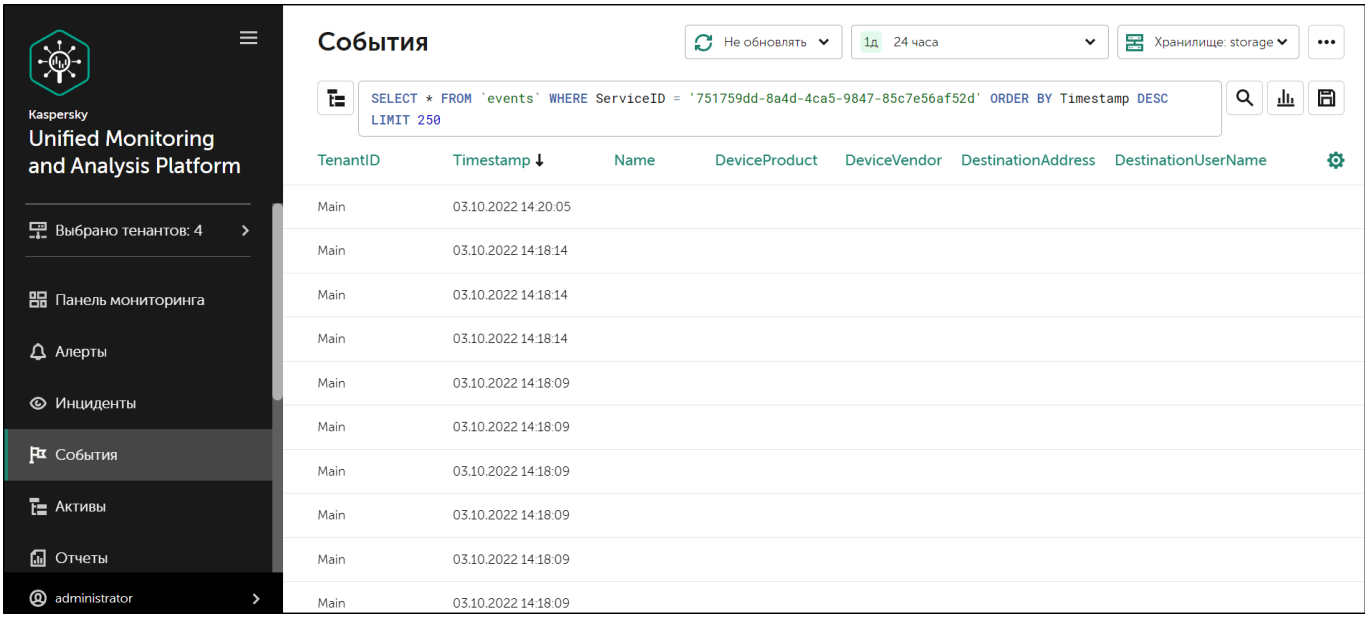
Вы можете искать события, обработанные определенным коррелятором или коллектором.

Чтобы найти события, относящиеся к коррелятору или коллектору:

1. Войдите в веб-интерфейс 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 значок 🔍.

   Отобразится таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса>`.



Результаты поиска событий

При поиске событий вы можете получить следующую ошибку о недоступности шарда:

```
Code: 279. DB::NetException: All connection tries failed. Log: \\n\\nTimeout exceeded
while connecting to socket (host.example.com:port, connection timeout 1000 ms)\\nTimeout
exceeded while connecting to socket (host.example.com:port, connection timeout 1000
ms)\\nTimeout exceeded while connecting to socket (host.example.com:port, connection
timeout 1000 ms)\\n\\n: While executing Remote. (ALL_CONNECTION_TRIES_FAILED) (version
23.8.8.207)\\n\"}",
```

В этом случае вам нужно переопределить параметры ClickHouse в параметрах хранилища.

Чтобы переопределить параметры ClickHouse:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы**.

2. В блоке **Конфигурация сервисов** → **Хранилища** нажмите на ресурс хранилища, который вы хотите изменить.

   Откроется окно **Редактирование хранилища**.

3. В поле **Переопределение параметров ClickHouse** укажите значения следующих параметров:

   - Чтобы пропускать недоступные шарды при поиске, вставьте следующие строки:
     ```
     <profiles>
             <default>
                     <skip_unavailable_shards>1</skip_unavailable_shards>
             </default>
     </profiles>
     ```

   - Чтобы определить объем используемой памяти, укажите значения параметров `max_server_memory_usage` или `max_memory_usage_for_all_queries` в соответствии с рекомендациями.

4. Чтобы применить параметры ClickHouse, нажмите на кнопку **Сохранить**.

5. Перезапустите сервисы хранилища, зависящие от этого ресурса.

   После этого ошибка о недоступности шарда будет устранена, и вы можете снова искать события, обработанные определенным коррелятором или коллектором.

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент KUMA, представляющий собой комплект настроек, на основе которых создаются и функционируют сервисы KUMA. Наборы ресурсов для сервисов 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 разделе веб-интерфейса KUMA **Ресурсы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы

- Корреляторы

- Хранилища
- Агенты

При выборе нужного типа открывается таблица с имеющимися наборами ресурсов для сервисов 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 веб-интерфейса KUMA, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища KUMA 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 хранилища в веб-интерфейсе KUMA**
2. **Создание сервиса хранилища в веб-интерфейсе KUMA**
3. **Установка узлов хранилища в сетевой инфраструктуре**

> При создании узлов кластера хранилища убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Запуск сервиса хранилища возможен, если разрешены форматы IPv6 и IPv4. Если вы работаете только с IPv4, укажите в поле `override configuration` ресурса `storage` следующее:

```
<interserver_listen_host>0.0.0.0</interserver_listen_host>
```

После изменения параметров хранилища его сервис 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:

- Улучшить 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 настройки** → **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 KUMA можно настроить перенос устаревших данных с кластера ClickHouse в холодное хранилище. 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 KUMA версии 4.2, не рекомендуется использовать HDFS в качестве холодного хранилища. Поддержка файловой системы HDFS будет прекращена в одном из будущих релизов. Пользователям, работающим с HDFS, рекомендуется запланировать переход на использование S3.

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.

Работа сервиса хранилища может нарушаться и его последующий запуск становится невозможным в следующих случаях:

- Если диск холодного хранения не настроен и на сервере в горячем хранилище закончилось место.
- Если диск холодного хранения настроен и на нем закончилось место.
- Если кластер не может получить доступ к настроенному диску холодного хранения.

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.
Сервис хранилища также необходимо перезапустить, если путь к хранилищу S3 был указан неправильно. 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 KUMA раз в 15 минут и после перезагрузки Ядра проверяет выполнение заданных условий хранения следующим образом:

1. KUMA получает партиции для проверяемого хранилища и группирует их по дискам холодного хранения и пространствам.
2. Для каждого пространства KUMA 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), KUMA 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 KUMA создает события аудита.

4. Если настроен срок хранения данных в KUMA, 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 KUMA, решение удаляет эти события или все партиции за самую старую дату.

   При удалении данных KUMA 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 KUMA **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 KUMA. 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 `<хост 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:

1. В веб-интерфейсе перейдите в раздел **Ресурсы** → **Хранилища** и выберите нужное хранилище.

2. В открывшемся окне в блоке параметров **Диски холодного хранения** в блоке параметров нужного диска нажмите на значок крестика, чтобы удалить диск.

3. В окне подтверждения нажмите **OK**.

   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 подсвечивается желтым цветом и отображается значок песочных часов. При запуске и окончании переноса данных создаются события аудита.

По завершении 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:

```
ROP 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 и S3-дисков), а затем удалить его из параметров хранилища.

Отключение, архивирование и подключение партиций

Если вы хотите оптимизировать дисковое пространство и ускорить выполнение запросов в KUMA, 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.

Вы также можете использовать созданные архивы с партициями в качестве резервных копий этих партиций.

Отключение партиций

Чтобы отключить партиции:

1. Выберите шард, на всех репликах которого вы планируете отключить партицию.

2. Получите идентификатор партиции с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/storage/<идентификатор хранилища>/deps/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 полученный идентификатор:

   ```
   sudo /opt/kaspersky/kuma/storage/<идентификатор хранилища>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<идентификатор партиции>'"
   ```

   Партиция отключена на всех репликах шарда. Теперь вы можете перенести данные 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 выполните архивирование:

```
sudo cd <путь к директории detached, содержащей отключенную партицию>
sudo zip -9 -r detached.zip *
```

Пример

```
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 решению:

1. В веб-интерфейсе откройте раздел **Ресурсы** → **Хранилище** и в параметрах используемого хранилища увеличьте значение параметра **Время хранения событий**.

   Данные удаляются в соответствии с датой, указанной в поле Timestamp (когда событие получено), и в соответствии со значением параметра **Время хранения событий**, которое вы задали для хранилища.

   Перед тем как выполнять восстановление архивных данных, убедитесь, что значение параметра **Время хранения событий** больше даты, указанной в поле Timestamp. В противном случае, архивные данные будут удалены в течение 1 часа.

2. Поместите архивную партицию в директорию `detached` вашего хранилища и распакуйте архив:

```
sudo unzip detached.zip -d <путь к директории detached>
```

Пример

```
sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-
d8d8e1eb3968/detached/
```

3. Подключите партицию с помощью команды:

```
sudo /opt/kaspersky/kuma/storage/<идентификатор хранилища>/deps/clickhouse/bin/client.sh -d kuma --multiline --
query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<идентификатор партиции>'"
```

4. Повторите шаги распаковки архива и подключения партиции на каждой реплике шарда.

Архивная партиция подключена, и события снова доступны для поиска.

Создание набора ресурсов для хранилища

Сервис хранилища в веб-интерфейсе KUMA создается на основе набора ресурсов для хранилища.

Чтобы создать набор ресурсов для хранилища в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA 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 можете 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 KUMA 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 мы рекомендуем указывать ограничение не более 90% включительно для всего хранилища или для отдельных пространств.

Мы не рекомендуем 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 KUMA 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 время хранения событий:

   - **Время хранения событий** – общая 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 KUMA.

     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 мы рекомендуем 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>

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.

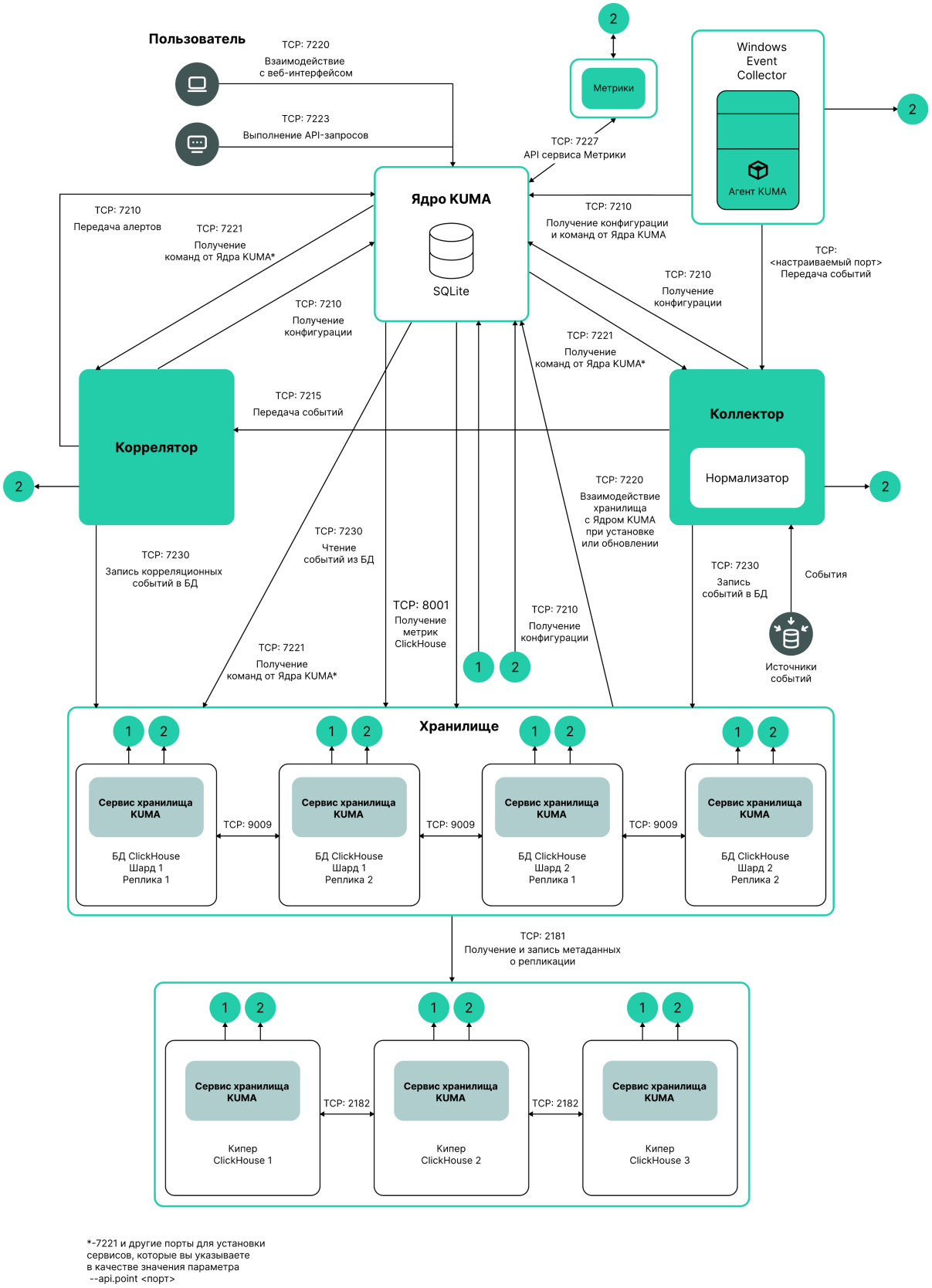


Схема распределенной установки

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 KUMA 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 мы рекомендуем 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 утеряны.

- 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 KUMA.

  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 мы рекомендуем 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 новый 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 KUMA.

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 KUMA.

    - В поле **Название** укажите название диска.

      Правила указания названия хранилища S3

      При указании названия хранилища S3 нужно выполнять следующие требования:

      - Название является уникальным в рамках одного хранилища.
      - Название состоит из строчных букв латинского алфавита и цифр. Вы также можете использовать в названии символ подчеркивания (_).

        Использование кириллических символов не допускается.
      - Название должно содержать от 1 до 128 символов в кодировке Unicode.

      > Вы не можете изменить название диска хранилища S3 без изменения пути к этому диску.

    - Если в качестве типа доменного имени диска вы выбрали **Локальный**, в поле **Путь** введите абсолютный путь директории смонтированного локального диска. Путь должен начинаться и оканчиваться символом "/".

      > Владельцем директории смонтированного локального диска должен быть пользователь KUMA.

    - 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 хранилища S3 (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**.

  - В поле **Цепочка сертификатов** укажите путь к файлу с полной цепочкой доверия сертификатов для подключения к хранилищу S3.

    Поле нужно заполнить, если для подключения к хранилищу S3 используется протокол HTTPS. Если используется HTTP, указывать сертификат не требуется. Файл должен содержать полную цепочку доверия сертификатов в формате BASE64, включая корневой сертификат, промежуточный (если используется) и сертификат хранилища S3.

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 исполнение файлов в указанной директории.

    - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например, /backup.

    - Имя 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, функции резервного копирования по расписанию, ручного резервного копирования, восстановления из резервной копии и импорта будут недоступны.

b. Если вы хотите настроить резервное копирование по расписанию, переведите переключатель **Резервное копирование по расписанию** в активное положение.

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**, KUMA установит ограничение в 128 МБ.

  Если ожидаемый трафик на сервис хранилища будет больше 1 Гбит/сек, мы рекомендуем 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 накапливается очередь запросов, воспользуйтесь рекомендациями по расчету и корректировке значения параметра **Размер буфера**, приведенными в статье Просмотр метрик KUMA 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 KUMA будет ждать заполнения буфера. Если буфер не заполнен, но указанное время прошло, KUMA 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. Мы рекомендуем использовать эту функцию только при условии, что у вас настроена балансировка на коллекторе и/или корреляторе: в коллекторе и/или корреляторе 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 (cpu, ram и т.д.) в виде дампов.

- В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте у Службы технической поддержки.

Набор ресурсов для хранилища создан и отображается в разделе **Ресурсы** → **Хранилища**. Теперь можно создать сервис хранилища.

Создание сервиса хранилища в веб-интерфейсе

Когда набор ресурсов для хранилища создан, можно перейти к созданию сервиса хранилища в KUMA.

Чтобы создать сервис хранилища в веб-интерфейсе KUMA:

1. В веб-интерфейсе 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 веб-интерфейсе KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор сервиса.

Установка хранилища в сетевой инфраструктуре KUMA

> Для корректной работы сервиса хранилища имя хоста сервера должно соответствовать одному из его IP-адресов. Проверьте соответствие в файле /etc/hosts. Список локальных IP-адресов можно просмотреть с помощью команды `ip a`.

Чтобы создать хранилище:

1. Войдите на сервер, на котором вы хотите установить сервис.

2. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --install
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --id XXXXX --install`

   > 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`.

3. Повторите шаги 1–2 для каждого узла хранилища.

   > На одном хосте может быть установлен только один сервис хранилища.

   Хранилище установлено.

Рекомендации по использованию системной памяти

Для регулирования потребления памяти при создании хранилища на системах с ограниченным объемом памяти рекомендуется определить объем используемой памяти и увеличить значение параметра `max_server_memory_usage`. Этот параметр определяет максимальный объем памяти, который может использовать сервер. Значение указывается в байтах.

По умолчанию для `max_server_memory_usage` устанавливается значение 0, при котором сервер может потреблять всю доступную память.

Значение параметра `max_server_memory_usage`, как правило, дополнительно ограничивается значением переменной `max_server_memory_usage_to_ram_ratio` (максимальный объем памяти для использования сервером, который выражается как отношение ко всей доступной памяти). Например, установленное по умолчанию значение 0.9 указывает на то, что сервер может потреблять 90% доступной памяти.

При определении объема используемой памяти нужно учитывать следующие ограничения:

- Оптимальное значение доступной системной памяти для использования хранилищем – 75% от общего объема памяти.

  Не рекомендуется использовать 100% доступной памяти. Это может привести к нехватке памяти при обработке поступающих запросов.

- Если на сервере установлены другие приложения, нужно выделить память для их работы.
- В случае изменения аппаратных параметров хост-сервера при последующем использовании хранилища нужно учитывать указанное значение параметра и корректировать его соответствующим образом.

Резервное копирование, восстановление и импорт партиций

В KUMA пользователям с ролью Главный администратор доступны следующие опции:

- Резервное копирование партиций по расписанию.
- Резервное копирование партиций вручную.
- Восстановление партиций из резервной копии.
- Импорт партиций из сторонней установки KUMA.

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 сторонней установки KUMA 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 веб-интерфейсе KUMA перейдите в раздел **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. Убедитесь, что у пользователя kuma есть права доступа к указанной директории.

      Если путь хранения не будет указан, выполнить резервное копирование будет невозможно.

   b. Переведите переключатель **Добавить автоматическое копирование** в активное положение.

   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 папку **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 веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** откройте действующее хранилище для настройки параметров.

2. В открывшемся окне **Редактирование хранилища** на вкладке **Основные параметры** в блоке **Настройка резервного копирования и восстановления** 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 исполнение файлов в указанной директории.
   - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например, /backup.
   - Имя 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 веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.

4. На панели инструментов или в меню (⋮) выберите **Резервное копирование** и нажмите **Создать резервную копию**.

   Опция **Создать резервную копию** доступна, если выбран один сервис хранилища в зеленом статусе.

Опция недоступна при следующих условиях:

- Если на предыдущем шаге вы установили флажок рядом с несколькими сервисами.
- Если сервис хранилища находится в красном статусе.
- 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 появившемся 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 папку **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.

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. Перенесите zip-файл резервной копии из директории **backup** в директорию **restore**.

2. Выдайте пользователю kuma права доступа к zip файлу резервной копии в папке restore с помощью следующей команды:

   ```
   sudo chown kuma *.zip
   ```

3. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.

4. На панели инструментов или в меню (⋮) выберите **Резервное копирование** → **Восстановить**.

5. В появившемся 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 появившемся 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.

Импорт партиций из сторонней установки KUMA

Импорт партиций из сторонней установки KUMA доступен пользователям с ролью Главный администратор.

Чтобы выполнить импорт партиций из сторонней установки KUMA:

1. Поместите zip-файл для импорта партиций в директорию **restore**. Из этой директории будет выполняться импорт партиций.

   Выдайте пользователю kuma права доступа к zip-файлу резервной копии в папке restore с помощью следующей команды:

   ```
   sudo chown kuma *.zip
   ```

2. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.

3. На панели инструментов или в меню (⋮) выберите **Резервное копирование** → **Импортировать**.

4. В появившемся окне **Импорт из сторонней установки KUMA** 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.

5. Нажмите **OK**.
6. В появившемся 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 сторонней установки KUMA выполнен.

Создание коррелятора

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий.

Действия в веб-интерфейсе KUMA

Создание коррелятора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы объединяются в набор ресурсов для коррелятора, а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

Чтобы создать коррелятор в веб-интерфейсе KUMA,

запустите мастер установки коррелятора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Создать коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

В результате выполнения шагов мастера в веб-интерфейсе KUMA 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 KUMA

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 веб-интерфейсе KUMA, 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 веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Добавить коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

Следуйте 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.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** создается набор ресурсов для коррелятора, а в разделе **Ресурсы** → **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 общие параметры коррелятора:

1. На вкладке **Основные параметры** заполните следующие поля:
   - В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - 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 другого тенанта, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и Общего тенантов.

- В поле **Обработчики** при необходимости укажите 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.

- В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

2. На вкладке **Дополнительные параметры** заполните следующие поля:

   - При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.

   - Переключатель **Периодическое создание дампа** используется по запросу техподдержки для генерации отчетов по потреблению ресурсов (cpu, ram и т.д.) в виде дампов.

   - В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте у техподдержки.

   - В поле **Число входящих запросов в очереди** укажите максимальное число запросов на вставку событий в базу данных, которые могут одновременно находиться в очереди на обработку коррелятором.

   Общие 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.

  - Должно содержать от 1 до 128 символов в кодировке Unicode.

  - Не может начинаться с символа $.

  - Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

  Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

  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. В вкладке мастера установки **Корреляция** следует выбрать или создать правила корреляции. В этих ресурсах задаются последовательности событий, указывающих на происшествия, связанные с безопасностью: при обнаружении таких последовательностей коррелятор создает корреляционное событие 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 KUMA.
  - **Изменение активного листа** – правило корреляции вносит изменения в активные листы.
  - **В коррелятор** – корреляционное событие отправляется на повторную обработку в то же правило корреляции.
  - **Изменение категории актива** – 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 хотите, чтобы алерт не создавался при срабатывании правила корреляции, но корреляционное событие все равно отправлялось в хранилище, установите флажки **В дальнейшую обработку** и **Не создавать алерт**. Если установлен только флажок **Не создавать алерт**, корреляционное событие не будет сохраняться в хранилище.
  - **Используются общие ресурсы** – 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.

С помощью кнопок **Поднять** и **Опустить** можно изменять положение выбранных правил корреляции в таблице правил корреляции, что отражается на последовательности 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 **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 **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 **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. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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.

- **словарь**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['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 применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

    - **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

    - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

    - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

      - **Символы на замену** – последовательность символов, которую требуется заменить.

      - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

    - **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

    - **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.

- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.

- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные

параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

- **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.

  Доступные параметры:

  - **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
  - **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.
  - **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Срок жизни кеша** – время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
  - **Кеш отключен** – с помощью этого переключателя можно включить или отключить кеширование. По умолчанию кеширование включено.

- **Обновление кеша 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 доступен начиная с KUMA 3.4.1. С помощью переключателя можно включить отправку коллектором KUMA рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения cybertrace-http. Этот тип возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.

  При обогащении через cybertrace коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в CyberTrace содержит квадратные скобки, например **[str1**, **str2]**), KUMA обрабатывает его как массив, а не как строку.

  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. Порт CyberTrace по умолчанию 9999.

  - **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. Значение по умолчанию: `1000`.

  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.

  - **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000.

  - **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. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- **cybertrace-http**

  Это новый тип потокового обогащения событий в CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять в системах с большим потоком событий. Производительность cybertrace-http превосходит показатели типа cybertrace.

  Ограничения:

  - Тип обогащения cybertrace-http неприменим для ретроспективного сканирования в KUMA.
  - В случае использования типа обогащения cybertrace-http обнаружения киберугроз не сохраняются в истории CyberTrace в окне Detections.

  Доступные параметры:

  - **Название** (обязательно) – уникальное название правила обогащения. Максимум 128 символов в кодировке Unicode.
  - **Тенант** (обязательно) – имя тенанта, в рамках которого вы планируете вести работу с CyberTrace.
  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443.
  - **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения.
  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
  - **Ключевые поля** (обязательно) – список полей событий, используемых для обогащения событий данными из CyberTrace.
  - **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000. По достижении 1 млн получаемых событий от сервера CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
  - **Основная версия CyberTrace** – выбор версии 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**.
  - **Отладка** – переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
  - **Теги** – теги для поиска ресурса.

- **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 сервиса, использующего 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 установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис 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.

- **проверка DLL Hijacking**

  DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак KUMA использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

  Для получения заключения KUMA отправляет запрос с информацией из полей события в KSN. В ответ на запрос KSN присылает результат анализа.

  Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или корреляторе.

  > 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** → **Обнаружение атак DLL Hijacking**).

Доступные параметры:

- **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.

- **Максимальный размер кеша** – максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`.

  Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если KUMA отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.

- **Максимальное количество событий в очереди обогащения** – при превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

- **Выполнять повторный запрос** – в ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса. Если этот параметр включен, настройте дополнительные параметры:

  - **Создавать дубликаты событий** – если этот параметр включен, KUMA создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.

    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.

    - Превышено значение, указанное в параметре **Количество запросов**.

    Если этот параметр выключен, KUMA продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.

    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.

    - Превышено значение, указанное в параметре **Количество запросов**.

  - **Количество запросов** – максимальное количество запросов в KSN. Если за указанное число запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.

  - **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.

  - **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

- **Прокси-сервер** – параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.

- **Сопоставление** – таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и списком соответствующих полей событий KUMA. Список параметров в запросе:

  - **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: OldFileHash.

  - **Путь до файла DLL** – полный путь, включающий имя файла; рекомендованное поле для сопоставления: OldFilePath. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

    Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

    Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

  - **Хеш процесса (md5)** – рекомендованное поле для сопоставления: FileHash.

  - **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

    Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

    Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

  - **Имя файла DLL** – рекомендованное поле для сопоставления: OldFileName.

  - **Имя процесса** – рекомендованное поле для сопоставления: FileName.

  - **Подпись процесса** – необязательный параметр; рекомендованное поле для сопоставления: FileID. В этом поле нужно указать поле KUMA, которое передает Organization из Subject подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.

  - **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**.

  Для каждого параметра укажите в таблице соответствующее ему поле события KUMA.

4. С помощью переключателя **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. Реагирование

Это необязательный шаг мастера установки. В 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 **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 **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 KUMA с Kaspersky Security Center. Задачи запускаются только на активах, импортированных из Kaspersky Security Center.

     Параметры реагирования

     - **Задача Kaspersky Security Center** (обязательно) – название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".

       Типы задач Kaspersky Security Center, которые можно запустить с помощью KUMA:

       - обновление;
       - поиск вирусов.

     - **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения:

       - SourceAssetID
       - DestinationAssetID
       - DeviceAssetID

     > Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

   - **Запуск скрипта** – правила реагирования для автоматического запуска скрипта. Например, вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA 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 корреляционных 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 корреляционных 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 KUMA 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 программы. 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 программу.

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 программы отобразится задача **Запустить программу**. 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 программы.

> 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/KATA** – 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 KUMA 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/KATA** – 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/KATA 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

4. В поле **Обработчики** укажите 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.

   Поле не обязательно для заполнения.

5. 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. В 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 решения.

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 **Сохранить**.

Выбранная точка назначения отображается в 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 решения.

   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 в кодировке Unicode.
   - 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 в кодировке Unicode. 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: 67 108 864 (64 МБ), в интерфейсе отображается как 0.

   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `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 верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке решения 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. Значение по умолчанию: `100`.

- **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.

- 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 **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 KUMA 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 новых сервисов коррелятора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри решения KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коррелятора следует установить на сервере, предназначенном для обработки событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите **Сохранить и создать сервис**.

На вкладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

Например:

/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

> Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

2. Закройте мастер, нажав **Сохранить**.

Сервис коррелятора создан в KUMA. Теперь сервис необходимо установить на сервере, предназначенном для обработки событий.

Установка коррелятора на сервере

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, 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 сервис.

2. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN сервера Ядра KUMA>:
<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется
порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --
api.port <порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример: `sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --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 веб-интерфейсе KUMA откройте раздел **Ресурсы** → **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 KUMA получает регулярно.

При обновлении, добавлении или удалении правила корреляции требуется обновить параметры коррелятора.

> Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из KUMA и обновить параметры коррелятора.

Создание коррелятора correlator-ng

Коррелятор correlator-ng – это компонент KUMA, предназначенный для корреляции и обработки событий из различных источников. Он позволяет фильтровать, объединять и анализировать события с помощью правил корреляции, селекторов и выражений.

> В KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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 KUMA 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 по порядку 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 конфигурации correlator-ng

> В KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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 запуска сервис устанавливает соединение с Ядром KUMA, получает конфигурацию правил и контейнеров и начинает обработку событий.

Коррелятор может быть развернут:

- на одном сервере;
- в кластере RAFT для обеспечения отказоустойчивости и масштабирования.

В этом разделе описывается структура конфигурации сервиса и назначение файлов конфигурации.

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 и 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.

Развертывание correlator-ng в кластере Raft

В KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического ознакомления. До выхода полнофункциональной версии коррелятора API методы, алгоритмы, синтаксис условий и другие функции и характеристики могут быть изменены.

Вы можете развернуть коррелятор correlator-ng в кластере Raft. Кластер обеспечивает синхронизацию состояния контейнеров корреляции между узлами и позволяет продолжать обработку событий при отказе отдельных узлов.

Рекомендуется использовать нечетное количество узлов для обеспечения отказоустойчивости.

Минимальное количество доступных узлов, необходимое для функционирования кластера, рассчитывается по формуле: *N / 2 + 1*, где N – общее количество узлов кластера. Например, при 3 узлах допустимое количество недоступных узлов – 1, при 5 узлах – 2, при 7 – 3.

Каждый узел коррелятора регистрируется в Ядре KUMA как отдельный сервис.

Параметры запуска коррелятора

Correlator-ng запускается через интерфейс командной строки и принимает набор параметров запуска.

Параметры запуска коррелятора

Параметр	Описание
`--id`	Уникальный идентификатор сервиса коррелятора.
`--core`	FQDN сервиса Ядра KUMA, например `https://kuma-core.example.com:7210`.
`--api.port`	API-порт коррелятора.
`--wd`	Рабочая директория коррелятора.
`--advertise.fqdn`	FQDN узла, который будет передан сервису Ядра KUMA для сетевого доступа к коррелятору.
`--advertise.api.port`	API-порт, который будет передан сервису Ядра KUMA.
`--san`	Список альтернативных имен для коррелятора.
`--http.client.connection.timeout`	Время ожидания HTTP-клиента при взаимодействии с микросервисами KUMA, в секундах. Значение по умолчанию – `10`.
`--logger.filter`	Уровень журналирования коррелятора. Возможные значения: `error`, `warn`, `info`, `debug`, `trace`. Значение по умолчанию – `info`.
`--threads.async`	Количество потоков для выполнения асинхронных операций (сетевые операции и обработка сигналов). Значение по умолчанию – `1`.

Параметры кластера Raft

Параметры кластера Raft

Параметр	Описание
`--raft.tick-interval`	Максимальный интервал времени реакции узла на изменения в кластере, в миллисекундах. Значение по умолчанию – `500`.
`--raft.heartbeat.tick`	Интервал обмена сообщениями между узлами кластера, в миллисекундах. Значение по умолчанию – `2`.
`--raft.election.tick`	Интервал времени, по истечении которого узел инициирует процедуру выбора управляющего узла, в миллисекундах. Значение по умолчанию – `2`.
`--raft.proposition.tick`	Количество интервалов времени перед отправкой накопленных изменений другим узлам кластера. Значение по умолчанию – `2`.
`--raft.proposition.max-size`	Максимальный размер пакета изменений, передаваемых другим узлам кластера, в мегабайтах. Значение по умолчанию – `4`.
`--raft.max-commited-size-per-tick`	Максимальный объем данных, принимаемых и обрабатываемых узлом за один интервал времени, в мегабайтах. Значение по умолчанию – `64`.
`--raft.request.timeout`	Время ожидания отправки Raft-запросов, в секундах. Значение по умолчанию – `10`.

Параметр	Описание
`--raft.entries-before-snapshot`	Количество записей в журнале Raft перед созданием снимка состояния. Значение по умолчанию – `1000`.
`--raft.shards`	Количество шардов Raft для распределения данных между группами. При изменении параметра требуется полный сброс состояния коррелятора. Значение по умолчанию – `4`.
`--raft.join`	FQDN узла кластера, к которому подключается новый узел коррелятора.

Дополнительные параметры

Дополнительные параметры

Параметр	Описание
`--suppress-alerts`	Отключает отправку корреляционных событий в сервис Ядра KUMA.

Развертывание первого узла

Перед созданием кластера необходимо запустить первый узел коррелятора correlator-ng.

Для запуска первого узла необходимо указать обязательные параметры:

- `--id` – уникальный идентификатор сервиса коррелятора;
- `--core` – FQDN сервиса Ядра KUMA;
- `--wd` – рабочая директория коррелятора;
- `--api.port` – API-порт коррелятора.

Пример запуска через интерфейс командной строки:

```
/opt/kaspersky/kuma/kuma ng correlator --id <идентификатор_сервиса_коррелятора> --core <FQDN_сервиса_Ядра_KUMA> --
wd <рабочая_директория_коррелятора> --api.port <API-порт_коррелятора>
```

После запуска в рабочей директории коррелятора создаются следующие директории:

- certificates
- config
- containers
- correlation

> После получения конфигурации от сервиса Ядра KUMA возможны ошибки, связанные со строгой типизацией выражений селекторов в правилах корреляции. В этом случае необходимо исправить ошибки в соответствующих YAML-файлах в директории config, следуя сообщениям об ошибках.

После успешного запуска первого узла и исправления возможных ошибок конфигурации можно приступать к развертыванию остальных узлов кластера.

Подключение узлов к кластеру Raft

Чтобы добавить узлы в кластер Raft:

1. Создайте рабочую директорию коррелятора:

```
mkdir /opt/correlator-wd
```

2. Скопируйте директорию config из рабочей директории первого узла коррелятора в рабочие директории остальных узлов.

3. Запустите correlator-ng с параметром подключения к кластеру `--raft.join`:

```
/opt/kaspersky/kuma/kuma ng correlator --wd <рабочая_директория_коррелятора> --api.port <API-порт_первого_узла_коррелятора> --id <идентификатор_сервиса_KUMA> --core <FQDN_сервиса_Ядра_KUMA> --raft.join <FQDN_первого_узла_коррелятора>:<API-порт_коррелятора_первого_узла>
```

   Команду запуска необходимо выполнить на каждом дополнительном узле коррелятора, изменяя параметры `--id` (уникальный идентификатор сервиса KUMA) и `--wd` (рабочую директорию узла коррелятора).

   Параметр `--raft.join` может указывать на любой узел, который уже входит в кластер. Необязательно указывать адрес первого узла коррелятора.

   Следует учитывать, что каждый узел коррелятора имеет собственный идентификатор сервиса KUMA. Поэтому для развертывания кластера необходимо создать соответствующее количество сервисов коррелятора в веб-интерфейсе KUMA. Все сервисы коррелятора должны быть созданы на основе одного и того же ресурса коррелятора.

Поддерживаемые типы данных correlator-ng

В KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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` и другие.

Поддерживаются следующие типы данных

Поддерживаемые типы данных

Тип данных	Описание
String	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

Тип данных	Описание
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 KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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
`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 KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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, позволяющие 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

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 по порядку 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 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 correlator-ng

> В KUMA 4.2 представлена бета-версия correlator-ng, которая предназначена для технического 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.
`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.

Функция	Описание
`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.

Функция	Описание
`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.

Функция	Описание
`hour(<timestamp>) -> 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.

Создание маршрутизатора событий

Маршрутизатор событий – это сервис, который позволяет принимать потоки событий от коллекторов и корреляторов и дальше распределять события по заданным точкам назначения в соответствии с настроенными фильтрами.

Чтобы события из коллектора были направлены в маршрутизатор событий, нужно создать ресурс точки назначения eventRouter с адресом маршрутизатора событий и привязать ресурс к тем коллекторам, которые должны отправлять события в маршрутизатор.

Маршрутизатор событий принимает события по API-порту, как и точки назначения типа storage и correlator.

Создать маршрутизатор можно в разделе **Ресурсы**.

Использование маршрутизатора событий позволяет снизить утилизацию каналов связи, что актуально для каналов с невысокой пропускной способностью и каналов, уже загруженных продуктивным трафиком.

Возможные сценарии использования:

Коллектор – маршрутизатор в дата-центре

Коллектор передает события на маршрутизатор в дата-центре, а маршрутизатор передает события в заданные точки назначения: коррелятор и хранилище.

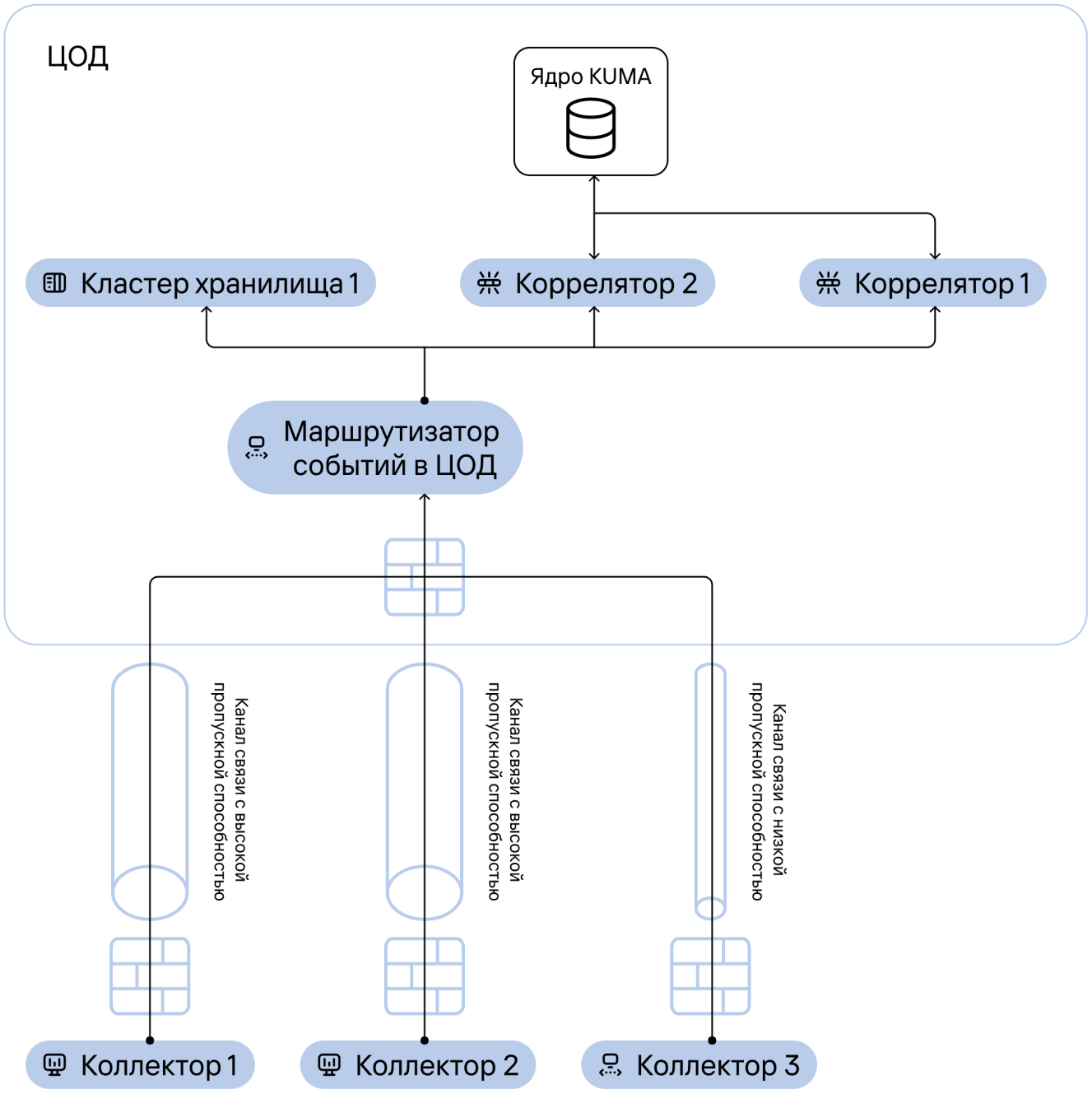


Схема подключения машрутизатора в дата-центре

Предусловия:

- В филиалах настроены коллекторы от KUMA 3.2.
- В дата-центре есть мощности для установки Маршрутизатора событий.
- В дата-центре установлена KUMA 3.2.

Шаги:

1. В дата-центре:

   a. Создать сервис **Маршрутизатор событий**.

   b. Создать точки назначения типов **storage** и **correlator** и указать их в Маршрутизаторе событий.

   c. В Маршрутизаторе событий на вкладке **Дополнительные параметры** настроить фильтр, чтобы передавать события в хранилище и/или коррелятор. Например, DeviceCustomString = correlator или DeviceCustomString = storage.

   d. Настроить обогащение.

2. В коллекторах филиалов:

   a. Создать точку назначения типа **eventRouter**.

   b. Указать URL Маршрутизатора событий в дата-центре офисе.

   c. Если eventRouter заменяет собой прежде настроенные точки назначения, их можно удалить.

Постусловие:

- Коллекторы в филиалах настроены.
- Маршрутизатор событий в дата-центре настроен.

Соединения филиалов с дата-центром оптимизированы: теперь не требуется в каждом коллекторе настраивать отправку событий и в хранилище, и в коррелятор в дата-центре, - таким образом нагрузка на канал связи будет снижена вдвое.

Маршрутизация в хранилище и коррелятор будет выполнена уже в дата-центре.

Каскадное подключение: несколько коллекторов – маршрутизатор в филиале, маршрутизатор в филиале – маршрутизатор в дата-центре

Несколько коллекторов передают события в маршрутизатор событий в филиале, маршрутизатор событий в филиале передает события в маршрутизатор в дата-центре, где уже происходит передача событий в заданные точки назначения: корреляторы и хранилище.

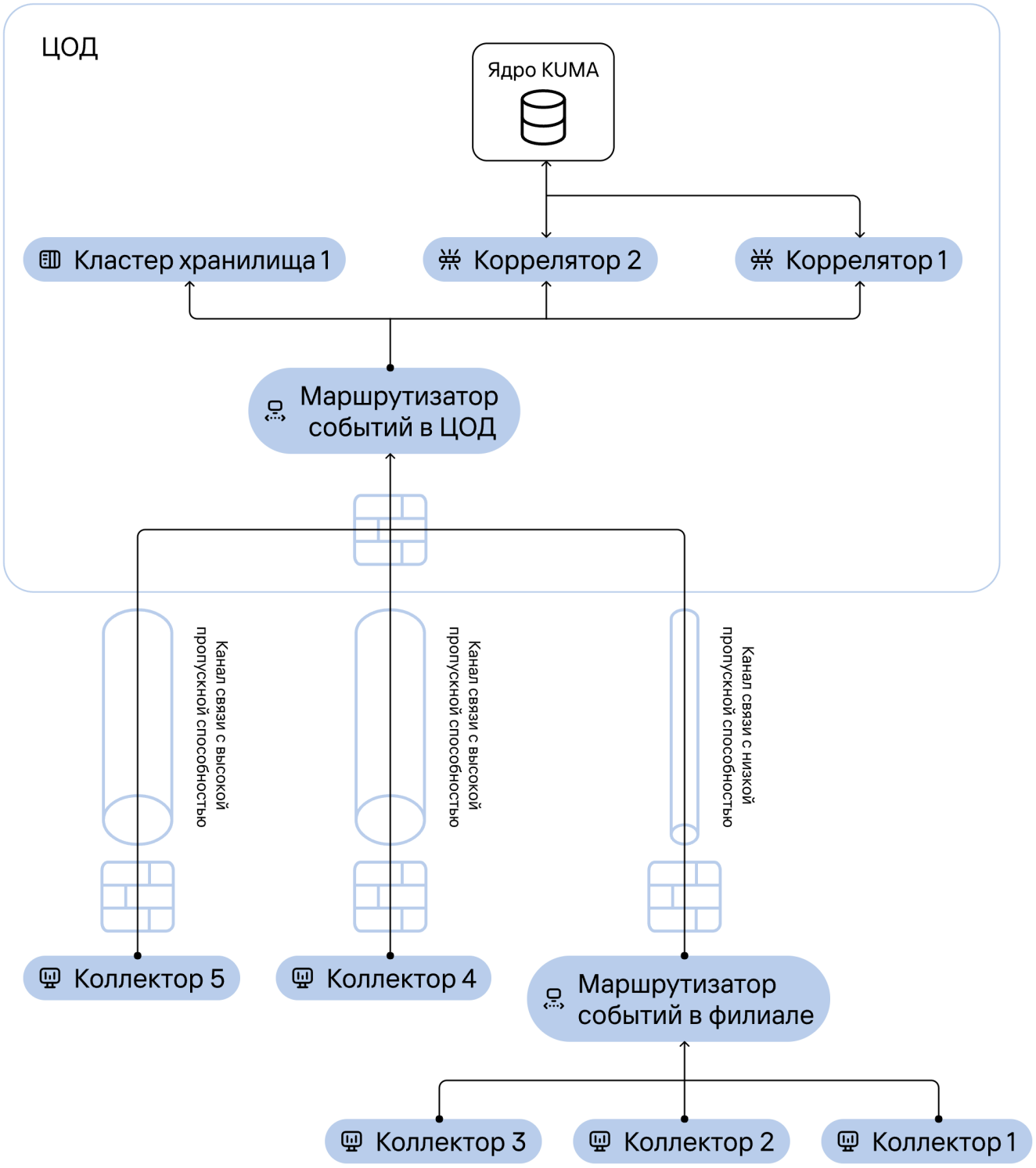


Схема каскадного подключения маршрутизаторов

Предусловия:

- В филиалах настроены коллекторы от KUMA 3.2.
- В дата-центре есть мощности для установки Маршрутизатора событий.
- В дата-центре установлена KUMA 3.2.

Шаги:

1. В дата-центре:

   a. Создать сервис **Маршрутизатор событий**.

   b. Создать Точки назначения типа **storage** и **correlator** и указать их в Маршрутизаторе событий.

   c. В Маршрутизаторе событий на вкладке **Дополнительные** параметры настроить фильтр, чтобы передавать события в хранилище и/или коррелятор. Например, DeviceCustomString = correlator или DeviceCustomString = storage.

2. В филиале:

   a. Создать сервис Маршрутизатор событий.

   b. Создать Точку назначения типа **eventRouter** и указать **URL** Маршрутизатора событий в дата-центре.

3. В коллекторах филиалов:

   a. Создать точку назначения типа **eventRouter** и указать **URL** Маршрутизатора событий в филиале.

   b. Если eventRouter заменяет собой прежде настроенные точки назначения, их можно удалить.

Постусловие:

1. Коллекторы в филиалах настроены.

2. Маршрутизатор событий в дата-центре и маршрутизатор событий в филиале настроены.

Соединение филиалов с дата-центром оптимизированы: теперь не требуется в каждом коллекторе настраивать отправку событий в дата-центр, достаточно собрать общий поток событий на маршрутизатор и одним потоком отправить в дата-центр.

Маршрутизатор событий доступен для установки только на устройства под управлением Linux. Создавать сервис может только пользователь с ролью Главный администратор. Создавать сервис можно в любом тенанте, привязка к тенанту не накладывает никаких ограничений.

Вы можете установить сервис маршрутизатора событий как на отдельном хосте, так и вместе с коллектором или коррелятором. Поскольку для маршрутизатора событий в файле инвентаря отсутствует отдельная секция, вы можете указать хост для установки маршрутизатора событий в секции `kuma_collector` или `kuma_correlator`. Также если вы планируете устанавливать маршрутизатор событий на отдельном хосте, вам нужно указать этот хост в файле инвентаря в секции `kuma_collector` или `kuma_correlator`, тогда при очередном обновлении KUMA сервис маршрутизатора событий также будет обновлен.

Для получения информации о параметрах работы сервиса доступны следующие метрики:

- IO
- Process
- OS

Как и для прочих ресурсов, для маршрутизатора событий в KUMA создаются следующие события аудита:

- Ресурс успешно добавлен.
- Ресурс успешно обновлен.
- Ресурс успешно удален.

Установка маршрутизатора событий состоит из двух этапов:

- Создание сервиса маршрутизатора событий в веб-интерфейсе KUMA с помощью мастера установки.
- Установка сервиса маршрутизатора событий на сервере.

Запуск мастера установки маршрутизатора событий

Чтобы запустить мастер установки маршрутизатора событий:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Маршрутизаторы событий**.
2. В открывшемся окне **Маршрутизаторы событий** нажмите **Добавить**.

Следуйте указаниям мастера установки.

Шаг 1. Общие параметры маршрутизатора событий

Это обязательный шаг мастера установки. На этом шаге вы указываете основные параметры маршрутизатора событий: название и тенант, которому он будет принадлежать.

Чтобы задать общие параметры маршрутизатора событий:

1. На вкладке **Основные параметры** заполните следующие поля:
   a. В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать маршрутизатор. Принадлежность маршрутизатора событий к тенанту носит организационный характер и не накладывает никаких ограничений.
   c. В поле **Обработчики** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество обработчиков соответствует количеству vCPU сервера, на котором установлен сервис.
   d. В поле **Описание** можно добавить описание сервиса: до 4000 символов в кодировке Unicode.

2. На вкладке **Дополнительные параметры** заполните следующие поля:

   a. При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.

   b. Переключатель **Периодическое создание дампа** используется по запросу Службы технической поддержки для генерации отчетов по потреблению ресурсов (cpu, ram и т.д.) в виде дампов.

   c. В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте у Службы технической поддержки.

Общие параметры маршрутизатора событий заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Маршрутизация

Это обязательный шаг мастера установки. Мы рекомендуем отправлять события как минимум в две точки назначения: в коррелятор для анализа и в хранилище для хранения. Также вы можете выбрать другой маршрутизатор событий в качестве точки назначения.

Чтобы задать параметры точки назначения, куда маршрутизатор событий будет направлять события, полученные от коллекторов:

1. В шаге мастера установки **Маршрутизация** нажмите **Добавить**.

2. В открывшемся окне **Создание точки назначения** задайте следующие параметры:

   a. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. С помощью переключателя **Состояние** вы можете при необходимости включить или выключить сервис.

   c. В раскрывающемся списке **Тип** выберите тип точки назначения. Доступны следующие значения:

      - nats-jetstream
      - tcp
      - http
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. На вкладке **Дополнительные параметры** укажите значения для параметров настройки. Набор параметров для настройки зависит от типа точки назначения, выбранного на вкладке **Основные параметры**. Более подробная информация о параметрах и значениях доступна по ссылке для каждого типа точки назначения в пункте c. этой инструкции.

Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Параметры маршрутизации настроены. Вы можете перейти к следующему шагу мастера установки.

Шаг 3. Проверка параметров

Это обязательный и заключительный шаг мастера установки.

Чтобы создать маршрутизатор событий в мастере установки:

1. Нажмите **Сохранить и создать сервис**.

   В нижней части окна отобразится команда, которая понадобится для установки маршрутизатора на сервере.

   Пример команды:

   ```
   /opt/kaspersky/kuma/kuma eventrouter --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса маршрутизатора событий> --api.port <порт, используемый для связи с сервисом> --install
   ```

   Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Следует убедиться в сетевой связности KUMA и при необходимости открыть порты, используемые компонентами решения.

2. Закройте мастер, нажав **Сохранить**.

Сервис будет установлен в веб-интерфейсе KUMA. Теперь вы можете перейти к установке сервиса в сетевой инфраструктуре KUMA.

Установка маршрутизатора событий на сервере

Чтобы установить маршрутизатор событий на сервере:

1. Войдите на сервер, на котором вы хотите установить сервис маршрутизатора событий.

   Если вы хотите установить сервис маршрутизатора событий на отдельном сервере, укажите хост в файле инвентаря в группе `kuma_correlator` и установите сервис маршрутизатора на этом хосте. При обновлении KUMA установщик выполнит обновление маршрутизатора, установленного на указанном в файле инвентаря хосте.

2. Создайте директорию /opt/kaspersky/kuma/.

3. Поместите в директорию /opt/kaspersky/kuma/ файл kuma, расположенный внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

4. 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
   ```

5. 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
   ```

6. Создайте пользователя kuma:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

7. Выдайте пользователю kuma права на директорию /opt/kaspersky/kuma и все файлы внутри директории:

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

8. Добавьте порт маршрутизатора событий KUMA в исключения брандмауэра.

> Для правильной работы решения убедитесь, что компоненты KUMA могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов KUMA.

9. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://<FQDN сервера Ядра KUMA>:
<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется
порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --
api.port <порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример:

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://kuma.example.com:7210 --id
XXXX --api.port YYYY --install
```

Маршрутизатор событий установлен на сервере. С его помощью можно получать события от коллекторов и перенаправлять события в заданные точки назначения.

Создание коллектора

Коллектор предназначен для приема сырых событий из источников событий, дальнейшей нормализации и передачи обработанных событий в точки назначения. Максимальный размер события, обрабатываемого коллектором KUMA: 4 МБ.

Если вы используете лицензию SMB и для коллектора превышено одновременно среднечасовое и среднесуточное количество EPS, допустимое лицензией, коллектор останавливает прием событий и отображается с красным статусом и уведомлением о превышении лимита EPS. Пользователю с ролью Главный администратор будет отправлено уведомление о превышении лимита EPS и остановке коллектора. Каждый час происходит подсчет среднечасового значения EPS и полученное значение сравнивается с лимитом EPS в лицензии. Если среднечасовое значение ниже лимита, ограничения на коллекторе будут сняты и коллектор восстановит прием и обработку событий.

Установка коллектора состоит из двух этапов:

- Создание коллектор в веб-интерфейсе KUMA с помощью мастера установки. На этом этапе вы задаете основные параметры настройки коллектора, которые будут применены во время установки коллектора на сервере.
- Установка коллектора на сервере сетевой инфраструктуры, предназначенном для получения событий.

Действия в веб-интерфейсе KUMA

Создание коллектора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы объединяются в набор ресурсов для коллектора, а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

Чтобы создать коллектор в веб-интерфейсе KUMA,

Запустите мастер установки коллектора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите на кнопку **Подключить источник**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

В результате выполнения шагов мастера в веб-интерфейсе KUMA 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 KUMA

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 веб-интерфейсе KUMA, 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 веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенной для получения событий. В мастере установки создается первая часть коллектора.

Чтобы запустить мастер установки коллектора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Подключить источник**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.

  Следуйте 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.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** создается набор ресурсов для коллектора, а в разделе **Ресурсы** → **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 общие параметры коллектора:

1. На вкладке **Основные параметры** заполните следующие поля:

   a. В поле **Название коллектора** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   > 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.

   b. 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 сервис. В сервис можно добавлять только ресурсы из выбранного и Общего тенантов.

c. В поле **Обработчики** при необходимости укажите 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.

d. В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

2. На вкладке **Дополнительные параметры** заполните следующие поля:

   a. При необходимости с помощью переключателя **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.

   b. Переключатель **Периодическое создание дампа** используется по запросу Службы технической поддержки для генерации отчетов по потреблению ресурсов (cpu, ram и т.д.) в виде дампов.

   c. В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте у Службы технической поддержки.

Общие 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 ↗.

Чтобы создать новый 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:

   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka

- http
- sql
- file
- 1c-log
- 1c-xml
- diode
- ftp
- nfs
- wmi
- wec
- etw
- snmp
- snmp-trap
- kata\edr
- vmware
- elastic
- office365
- dfi
- universalAPI

При использовании типа коннектора **tcp** или **udp** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса устройств, с которых были получены события.

При использовании типа коннектора **wmi**, **wec** или **etw** 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 KUMA 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** → **Коннекторы**.

Перейдите к следующему шагу мастера установки.

Шаг 3. Парсинг событий

Это обязательный шаг мастера установки. На вкладке мастера установки **Парсинг событий** вам нужно нажать на кнопку **+ Добавить парсинг событий**, после чего в открывшемся окне **Основной парсинг событий** в раскрывающемся списке **Нормализатор** выбрать или создать нормализатор. В параметрах нормализатора необходимо определить 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 нормализатор по умолчанию сохраняется в наборе ресурсов для коллектора. Вы не можете использовать созданный нормализатор в других коллекторах. Вы можете установить флажок **Сохранить нормализатор**, чтобы создать нормализатор в виде отдельного ресурса. В этом случае нормализатор будет доступен для выбора в других коллекторах тенанта.

Добавление нормализатора в набор ресурсов

Чтобы добавить нормализатор в набор ресурсов:

1. Нажмите на кнопку **+ Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора. По умолчанию будет выбрана вкладка **Схема нормализации**.

2. В раскрывающемся списке **Нормализатор** выберите нормализатор. Вы можете выбрать нормализатор, который принадлежит тенанту коллектора или Общему тенанту.

   Отобразятся параметры нормализатора.

   Если вы хотите изменить параметры нормализатора, в раскрывающемся списке **Нормализатор** нажмите на значок карандаша (✎) рядом с названием нормализатора и в открывшемся окне **Редактирование нормализатора** нажмите на темный кружок. Откроется окно **Основной парсинг событий** с параметрами нормализатора. Если вы хотите настроить параметры дополнительного парсинга, в окне **Редактирование нормализатора** наведите курсор на темный кружок и нажмите на отобразившийся значок плюса. Откроется окно **Дополнительный парсинг событий** с параметрами дополнительного парсинга. Подробнее о настройке параметров дополнительного парсинга событий см. ниже в разделе **Создание структуры правил нормализации событий**.

3. Нажмите на кнопку **OK**.

Нормализатор будет добавлен и отобразится в виде темного кружка на вкладке мастера установки **Парсинг событий**. Вы можете нажать на темный кружок, чтобы просмотреть параметры нормализатора.

Чтобы создать в коллекторе новый нормализатор:

1. Нажмите на кнопку **+ Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора. По умолчанию будет выбрана вкладка **Схема нормализации**.

2. Если хотите создать нормализатор в виде отдельного ресурса, установите флажок **Сохранить нормализатор**. Если флажок установлен, нормализатор будет доступен для выбора в других коллекторах тенанта. По умолчанию флажок снят.

3. В поле **Название** введите уникальное имя нормализатора. Максимальная длина имени: до 128 символов в кодировке Unicode.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбранного значения вы можете использовать преднастроенные правила сопоставления полей событий или указать правила вручную. При выборе определенных методов парсинга могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

   Доступные методы 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 вы можете обращаться к полям вложенных объектов, указывая названия параметров поочередно через точку. 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 неправильно.

     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 обрабатываемое событие целиком передается в дополнительный нормализатор.

     В качестве разделителя строк вы можете использовать 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** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

   - **cef**

     Этот метод парсинга используется для обработки данных в формате CEF.

     При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

   - **regexp**

     Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений.

     Вам нужно добавить регулярное выражение (синтаксис RE2) с именованными группами захвата в поле блока параметров **Нормализация**. Имя группы захвата и ее значение будут считаться полем и значением сырого события, которое можно будет преобразовать в поле события формата KUMA.

Чтобы добавить правила обработки событий:

1. При необходимости в поле **Примеры событий** скопируйте пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например `"(?P<name>regexp)"`. Регулярное выражение, добавленное в поле блока параметров **Нормализация**, должно полностью совпадать с событием. При разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: `^`, `$`.

   Вы можете добавить несколько регулярных выражений или удалить регулярные выражения. Для добавления регулярного выражения нажмите на кнопку **Добавить регулярное выражение**. Для удаления регулярного выражения нажмите рядом с ним на значок удаления ✕.

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Вы можете выбрать соответствующее группе захвата поле KUMA в столбце напротив каждой группы захвата. Если вы именовали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий будут добавлены.

- **syslog**

  Этот метод парсинга используется для обработки данных в формате syslog.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

  Для парсинга событий в формате rfc5424 с секцией `structured-data` вам нужно в раскрывающемся списке **Сохранить дополнительные поля** выбрать **Да**. В этом случае значения из секции `structured-data` станут доступны в полях `Extra`.

- **csv**

  Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

  При выборе этого метода парсинга вам нужно в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя значений в строке можно использовать любой однобайтовый символ ASCII.

- **kv**

  Этот метод парсинга используется для обработки данных в формате ключ-значение. Доступные параметры метода парсинга описаны в таблице ниже.

Доступные параметры метода парсинга

Параметр	Описание
Разделитель пар	Символ для разделения пар ключ-значение. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель значений**.
Разделитель значений	Символ для разделения ключа и значения. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель пар**.

- **xml**

  Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

  Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

  При выборе этого метода парсинга вы можете указать ключевые атрибуты XML, которые требуется извлекать из тегов, в блоке параметров **Атрибуты XML**. Если в структуре XML в одном теге есть атрибуты XML с разными значениями, вы можете определить значение, указав ключ к значению в столбце **Исходные данные** таблицы **Сопоставление**.

  Чтобы добавить ключевые атрибуты XML:

  1. Нажмите на кнопку **+ Добавить поле**.

  2. В открывшемся окне укажите путь к атрибуту XML.

  Вы можете добавить несколько атрибутов XML и удалить атрибуты XML. Для удаления отдельного атрибута XML нажмите рядом с ним на значок удаления ✕. Для удаления всех атрибутов XML нажмите на кнопку **Сбросить**.

  Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

  Нумерация тегов

  Начиная с версии KUMA 2.1.3 доступна автоматическая нумерация тегов в событиях в формате XML. Это позволяет распарсить событие с одинаковыми тегами или неименованными тегами, такими как `<Data>`.

  В качестве примера мы используем нумерацию тегов атрибута `EventData` **события Microsoft Windows PowerShell event ID 800**.

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="
    {0e8478c5-3605-4e8c-8497-1e730c959516}" EventSourceName="NTDS" />
    <EventID Qualifiers="0000">0000</EventID>
    <Version>@</Version>
    <Level>4</Level>
    <Task>15</Task>
    <Opcode>0</Opcode>
    <Keywords >0x8080000000000000</Keywords>
    <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
    <EventRecordID>55647</EventRecordID>
    <Correlation />
    <Execution ProcessID="1" ThreadID="1" />
    <Channel>service</Channel>
    <Computer>computer</Computer>
    <Security UserID="0000" />
  </System>
  <EventData>
    <Data>583</Data>
    <Data>36</Data>
```

```
    <Data>192.168.0.1:5084</Data>
    <Data>level</Data>
    <Data>name, lDAPDisplayName</Data>
    <Data />
    <Data>5545</Data>
    <Data>3</Data>
    <Data>0</Data>
    <Data>0</Data>
    <Data>0</Data>
    <Data>15</Data>
    <Data>none</Data>
  </EventData>
</Event>
```

Для парсинга событий с одинаковыми тегами или неименованными тегами вам нужно настроить нумерацию тегов и маппинг данных для пронумерованных тегов с полями события KUMA.

KUMA 3.0.x поддерживает одновременное использование атрибутов XML и нумерации тегов в рамках одного экстранормализатора. Если атрибут XML содержит неименованные теги или одинаковые теги, мы рекомендуем использовать нумерацию тегов. Если атрибут XML содержит только именованные теги, мы рекомендуем использовать атрибуты XML.

Для использования атрибутов XML и нумерации тегов в экстранормализаторах вам нужно последовательно включить параметр **Использовать сырое событие** в каждом экстранормализаторе по пути следования события в целевой экстранормализатор и в целевом экстранормализаторе.

В качестве примера работы нумерации тегов вы можете обратиться к нормализатору **MicrosoftProducts**. Параметр **Использовать сырое событие** включен последовательно в экстранормализаторах **AD FS** и **424**.

Чтобы настроить парсинг событий с неименованными или одинаковыми тегами:

1. Откройте существующий или создайте новый нормализатор.

2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите **xml**.

3. В поле **Нумерация тегов** нажмите на кнопку **+ Добавить поле**.

4. В отобразившемся поле укажите полный путь к тегу, элементам которого требуется присвоить порядковый номер, например `Event.EventData.Data`. Первому тегу будет присвоен номер 0. Если тег пустой, например `<Data />`, ему также будет присвоен порядковый номер.

5. Для настройки маппинга данных в группе параметров **Сопоставление** нажмите на кнопку **+ Добавить строку** и выполните следующие действия:

   a. В отобразившейся строке в поле **Исходные данные** укажите полный путь к тегу и индекс тега. Например, для события Microsoft Windows PowerShell event ID 800 из примера выше полные пути к тегам и индексы тегов будут выглядеть следующим образом:

      - `Event.EventData.Data.0`;
      - `Event.EventData.Data.1`;
      - `Event.EventData.Data.2` и так далее.

   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии KUMA, в которое попадет значение из пронумерованного тега после выполнения парсинга.

6. Сохраните изменения одним из следующих способов:

   - Если вы создали новый нормализатор, нажмите на кнопку **Сохранить**.
   - Если вы изменили существующий нормализатор, в коллекторе, к которому привязан нормализатор, нажмите на кнопку **Обновить параметры**.

Настройка парсинга будет завершена.

- **netflow**

  Этот метод парсинга используется для обработки данных во всех поддерживаемых форматах на основе протокола NetFlow: NetFlow v5, NetFlow v9 и IPFIX.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. При этом будут учтены исходные поля всех версий NetFlow (NetFlow v5, NetFlow v9 и IPFIX).

  Если метод парсинга **netflow** выбран для основного парсинга, дополнительная нормализация недоступна.

  > В правилах сопоставления по умолчанию для метода парсинга **netflow** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow5**

  Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

> В правилах сопоставления по умолчанию для метода парсинга **netflow5** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow9**

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow9** выбран для основного парсинга, дополнительная нормализация недоступна.

  > В правилах сопоставления по умолчанию для метода парсинга **netflow9** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sflow5**

  Этот метод парсинга используется для обработки данных в формате sflow5.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **sflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

- **ipfix**

  Этот метод парсинга используется для обработки данных в формате IPFIX.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна.

  > В правилах сопоставления по умолчанию для метода парсинга **ipfix** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sql**

  Нормализатор использует этот метод парсинга для обработки данных, полученных с помощью выборки из базы данных.

  Этот метод парсинга становится доступным, только если на шаге Транспорт мастера установки вы указали коннектор с типом sql.

- **normalizer**

  Этот метод парсинга позволяет переиспользовать ранее созданный нормализатор в качестве основного или дополнительного для обработки событий.

  При выборе этого метода парсинга вам нужно в раскрывающемся списке **Нормализатор** выбрать один из ранее созданных нормализаторов с типом json, cef, regexp, syslog, csv, kv, xml или sql. Нормализаторы с методом парсинга **normalizer** недоступны для выбора.

5. В раскрывающемся списке **Сохранить исходное событие** выберите, требуется ли сохранять исходное сырое событие в повторно созданном нормализованном событии:

   - **Не сохранять** – не сохранять исходное событие. Это значение выбрано по умолчанию.

   - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Вы можете использовать это значение при отладке сервиса. В этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок.

   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

6. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не было настроено сопоставление (см. шаг 8 этой инструкции):

   - **Нет**. Это значение выбрано по умолчанию.

   - **Да**. Поля исходного события сохраняются в поле `Extra` нормализованного события.

   Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

7. При необходимости в поле **Примеры событий** укажите пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

   Вы можете добавить несколько примеров событий. Каждый новый пример нужно указывать с новой строки. При этом в таблице **Сопоставление** его результат парсинга отобразится в столбце **Примеры**. Это позволяет проверить правильность сопоставления полей для разных типов входящих событий.

   Ограничения при парсинге примеров событий

   При парсинге примеров данных, указанных в поле **Примеры событий**, в дополнительном нормализаторе не учитываются следующие параметры:

   - обогащение, настроенное в корневом нормализаторе;

   - фильтры, заданные в дополнительном нормализаторе;

   - значение параметра **Использовать сырое событие**;

   - преобразования в корневом нормализаторе;

   - преобразования для значения параметра **Поле, которое следует передать в нормализатор**.

   Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

8. В таблице **Сопоставление** настройте сопоставление полей исходного события с полями событий KUMA:

   a. Нажмите на кнопку **+ Добавить строку**.

   Вы можете добавить несколько строк таблицы или удалить строки таблицы. Для удаления строки таблицы установите рядом с ней флажок и нажмите на кнопку **Удалить**.

   b. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите сопоставить с полем события KUMA.

   Подробнее о формате названий полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

   Если вы хотите создать правила изменения полей исходного события перед записью в поля событий KUMA, нажмите на значок настройки (⚙) рядом с названием поля и в открывшемся окне **Преобразование** нажмите на кнопку **+ Добавить преобразование**. Вы можете изменить порядок правил и удалить правила. Для изменения порядка правил используйте значки изменения порядка (⠿). Для удаления правила нажмите рядом с ним на значок удаления (✕).

   Доступные преобразования

   Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

   - **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

   - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

   - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

     - **Символы на замену** – последовательность символов, которую требуется заменить.

     - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

   - **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

   - **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.

- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.

- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

Если на шаге Транспорт мастера установки вы указали коннектор с типом file, 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.

Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.

c. В столбце **Поле KUMA** в раскрывающемся списке выберите поле события KUMA. Вы можете найти поле события KUMA, введя его названия. Если название поля события KUMA начинается с `DeviceCustom*` и `Flex*`, при необходимости в поле **Подпись** укажите уникальную пользовательскую метку.

Если вы хотите, чтобы KUMA могла выполнить обогащение событий данными об активах и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам нужно настроить сопоставление полей для адреса хоста и имени хоста в зависимости от назначения актива. Например, вы можете настроить сопоставление для полей событий KUMA **SourceAddress** и **SourceHostName**, или **DestinationAddress** и **DestinationHostName**. В результате обогащения в карточке события появится поле события KUMA **SourceAssetID** или **DestinationAssetID** и ссылка, по которой можно будет перейти в карточку актива. В результате обогащения сведения об активе также будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

Таблица **Сопоставление** недоступна, если в поле **Метод парсинга** выбрано значение **normalizer**.

9. Нажмите на кнопку **OK**.

Нормализатор будет создан и отобразится в виде темного кружка на вкладке мастера установки **Парсинг событий**. Вы можете нажать на темный кружок, чтобы просмотреть параметры нормализатора. Если вы хотите настроить параметры дополнительного парсинга наведите курсор на темный кружок и нажмите на отобразившийся значок плюса. Откроется окно **Дополнительный парсинг событий** с параметрами дополнительного парсинга. Подробнее о настройке параметров дополнительного парсинга событий см. ниже в разделе **Создание структуры правил нормализации событий**.

При отображении схемы нормализации структура вложенных нормализаторов не отображается. Чтобы ее просмотреть, нужно перейти в карточку нормализатора по ссылке с его названием. Если вы используете вложенный нормализатор с дополнительной нормализацией, нужно учитывать, что структура выходных данных может меняться. В этом случае важно понимать, какое поле будет передаваться другому дополнительному нормализатору.

Обогащение нормализованного события дополнительными данными

Вы можете создавать в нормализаторе правила обогащения, чтобы добавлять дополнительные данные в созданные нормализованные события. Правила обогащения хранятся в нормализаторе, в котором они были созданы.

Вкладка **Обогащение** недоступна, если на вкладке **Схема нормализации** в поле **Метод парсинга** выбрано значение **normalizer**.

Чтобы добавить правила обогащения в нормализатор:

1. Выберите основное или дополнительное правило нормализации и в открывшемся окне выберите вкладку **Обогащение**.

2. Нажмите на кнопку + **Добавить обогащение**.

   Отобразится блок параметров правила обогащения. Вы можете добавить несколько правил обогащения или удалить правила обогащения. Для удаления правила обогащения нажмите рядом с ним на значок удаления (✕).

3. В раскрывающемся списке **Исходный тип** выберите тип источника обогащения. При выборе определенных типов источника обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

   Доступные типы источников обогащения:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже.

     Доступные параметры типа обогащения

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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.

   - **словарь**

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже.

     Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

     Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

- **таблица**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события KUMA, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий KUMA, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

- **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое требуется поместить данные. Вы не можете выбрать значение, если в раскрывающемся списке **Исходный тип** вы выбрали **таблица**.

5. Если вы хотите включить детализацию в журнале нормализатора, включите переключатель **Отладка**. По умолчанию переключатель выключен.

6. Нажмите на кнопку **OK**.

Правила обогащения событий дополнительными данными будут добавлены в нормализатор в выбранное правило парсинга.

Настройка парсинга с привязкой к IPv4-адресам

Если на шаге Транспорт мастера установки вы указали коннектор с типом udp, tcp или http, вы можете направить события с нескольких IPv4-адресов от источников разных типов в один коллектор, и коллектор применит указанные нормализаторы. Для этого вам нужно указать несколько IPv4-адресов и выбрать нормализатор, который требуется использовать для событий, поступающих с указанных IPv4-адресов. Доступны следующие типы нормализаторов: **json**, **cef**, **regexp**, **syslog**, **csv**, **kv**, **xml** и **normalizer**.

Если в коллекторе с настроенными нормализаторами и привязкой к IPv4-адресам вы выберите тип коннектора, отличный от **upd**, **tcp** или **http**, вкладка **Настройки парсинга** перестанет отображаться и на вкладке мастера установки **Парсинг событий** будет указан только первый из ранее указанных нормализаторов. Вкладка **Настройки парсинга** перестанет отображаться сразу, изменения будут применены после сохранения ресурса. Если вы хотите вернуться к прежним параметрам, выйдите из мастера установки без сохранения.

Для нормализаторов с типом **Syslog** и **regexp** допускается использование цепочки нормализаторов. В этом случае вы можете указать дополнительные условия нормализации в зависимости от значения поля **DeviceProcessName**. В отличие от дополнительной нормализации вы можете указывать общедоступные нормализаторы.

Чтобы настроить парсинг с привязкой к IPv4-адресам:

1. Выберите вкладку **Настройки парсинга** и нажмите на кнопку **+ Источник события**.

   Отобразится блок параметров парсинга. Вы можете добавить несколько парсингов или удалить парсинги. Для удаления парсинга нажмите рядом с ним на значок удаления (×).

2. В поле **IP-адрес(-а)** введите IPv4-адрес, с которого будут поступать события. Вы можете ввести несколько IPv4-адресов через запятую. Длина списка IPv4-адресов не ограничена, но мы рекомендуем указывать ограниченное количество IPv4-адресов для соблюдения баланса нагрузки на коллектор. Вам нужно указать значение в этом поле, если вы хотите применять несколько нормализаторов в одном коллекторе.

   > IPv4-адрес должен быть уникальным для каждого нормализатора. KUMA выполняет проверку уникальности IPv4-адресов и если вы укажете одинаковый IPv4-адрес для разных нормализаторов, отобразится сообщение `Поле должно быть уникальным`.

   Если вы планируете отправлять все события в один нормализатор без указания IPv4-адресов, мы рекомендуем создать отдельный коллектор. Для повышения производительности мы рекомендуем создать отдельный коллектор с одним нормализатором, если вы хотите применить один нормализатор к событиям с большого количества IPv4-адресов.

3. В раскрывающемся списке **Нормализатор** создайте или выберите нормализатор. Вы можете нажать на значок стрелки рядом с раскрывающимся списком, чтобы выбрать вкладку **Схемы парсинга**.

   Нормализация будет срабатывать, если на шаге Транспорт мастера установки вы указали коннектор с типом udp, tcp или http. При этом для коннектора с типом **http** должен быть указан заголовок (англ. header) источника событий. С учетом доступных коннекторов, следующие типы нормализатора доступны для автоматического распознавания источников: **json**, **cef**, **regexp**, **syslog**, **csv**, **kv** и **xml**.

4. Если вы выбрали нормализатор с типом **Syslog** или **regexp** и вы хотите добавить условную нормализацию, нажмите на кнопку **+ Добавить условную нормализацию**. Условная нормализация будет доступна, если в основном нормализаторе в таблице **Сопоставление** вы настроили сопоставление поля исходного события с полем события KUMA **DeviceProcessName**. В группе параметров **Условие** в поле **DeviceProcessName** укажите имя процесса и в раскрывающемся списке создайте или выберите нормализатор. Вы можете указать несколько комбинаций поля события KUMA **DeviceProcessName** и нормализатора. Нормализация будет выполняться до первого совпадения.

Парсинг с привязкой к IPv4-адресам будет настроен.

Создание структуры правил нормализации событий

Для реализации сложной логики обработки событий вы можете добавить в нормализатор несколько правил парсинга событий. События передаются между правилами парсинга событий в зависимости от указанных условий. События обрабатываются последовательно в соответствии с порядком создания правил парсинга. Путь обработки события отображается в виде стрелочек.

Чтобы создать дополнительное правило парсинга:

1. Создайте нормализатор. Подробнее о создании нормализаторов см. выше в разделе **Добавление нормализатора в набор ресурсов**.

   Созданный нормализатор отобразится в виде темного кружка на вкладке мастера установки **Парсинг событий**.

2. Наведите курсор на темный кружок и нажмите на отобразившийся значок плюса.

3. В открывшемся окне **Дополнительный парсинг события** укажите 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 **Да**. Значение по умолчанию: **Нет**. Мы рекомендуем передавать сырое событие в нормализаторы с типами **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 **Да**.

     Если вы хотите отправлять в дополнительный нормализатор только события с определенным полем, в поле **Поле, которое следует передать в нормализатор** укажите порт.

     На этой вкладке вы можете определить другие условия, при выполнении которых событие будет поступать на дополнительный парсинг.

   - Вкладка **Схема нормализации**:

     На этой вкладке вы можете настроить правила обработки событий, по аналогии с параметрами основного нормализатора. Параметр **Сохранить исходное событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании нормализатора.

   - Вкладка **Обогащение**:

     На этой вкладке вы можете настроить правила обогащения событий. Подробнее о настройке правил обогащения см. выше в разделе **Обогащение нормализованного события дополнительными данными**. Эта вкладке недоступна, если на вкладке **Схема нормализации** в поле **Метод парсинга** выбрано значение **normalizer**.

4. Нажмите на кнопку **OK**.

Дополнительное правило парсинга будет добавлено в нормализатор и отобразится в виде темного блока. В темном блоке указаны условия, при которых дополнительное правило парсинга будет задействовано.

Вы можете выполнить следующие действия:

- Изменить параметры дополнительного правила парсинга, нажав на него.
- Найти дополнительное правило парсинга, введя его название в поле в верхней части окна.
- Создать новое дополнительное правило парсинга. Для этого наведите курсор на дополнительное правило парсинга и нажмите на отобразившийся значок плюса.
- Дублировать дополнительное правило парсинга. Для этого наведите курсор на дополнительное правило парсинга и нажмите на значок дублирования ( ).
- Удалить дополнительное правило парсинга. Для этого наведите курсор на дополнительное правило парсинга и нажмите на значок корзины.

- Изменить расположение и последовательность дополнительных нормализаторов. Для этого установите флажок рядом с дополнительным нормализатором и в панели инструментов нажмите **Переместить**. В открывшемся окне **Перенести нормализатор** выберите нужные значения в раскрывающихся списках **Новый родительский нормализатор** и **Вставить после нормализатора** и нажмите **Сохранить**. Если значение в раскрывающемся списке **Вставить после нормализатора** не выбрано, дополнительный нормализатор будет перенесен в самое начало последовательности дополнительных нормализаторов в выбранном родительском нормализаторе. В нижней части блока дополнительного нормализатора указывается количество связанных с ним дополнительных нормализаторов.

  Вы можете одновременно перемещать несколько дополнительных нормализаторов одного уровня. Если вы перемещаете дополнительный нормализатор, у которого есть дочерние нормализаторы, переместится вся цепочка.

- Регулировать отображение структуры правил нормализации в панели инструментов с помощью кнопок **Свернуть по умолчанию**, **Развернуть все**, **Компактный вид**.

  По умолчанию сворачиваются все дополнительные нормализаторы, начиная со второго уровня. Основной нормализатор – это нулевой уровень, затем следует первый уровень дополнительных нормализаторов, остальные уровни дополнительных нормализаторов будут свернуты. При переходе к схеме нормализации отображается схема, свернутая по умолчанию. Для каждого элемента в дереве нормализаторов вы можете сворачивать и разворачивать дочерние элементы с помощью значков **Свернуть** ( ) и **Развернуть** ( ). Значки появляются, если навести курсор мыши на родительский нормализатор.

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.

Мы рекомендуем придерживаться выбранной схемы нормализации, когда вы указываете фильтры. Используйте в фильтрах только служебные поля KUMA и те поля, которые вы указали в нормализаторе в разделе **Сопоставление** и **Обогащение**. Например, если в нормализации не используется поле DeviceAddress, избегайте использования поля DeviceAddress в фильтре - такая фильтрация не сработает.

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 в кодировке Unicode.

4. В разделе **Условия** задайте условия, которым должны соответствовать отсеиваемые события:

- С помощью кнопки **Добавить условие** добавляются условия фильтра, можно выбрать два значения (левый и правый операнды) и назначить операцию, которую вы 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. В результате выбора появляются дополнительные параметры, с помощью которых необходимо точно определить значение, которое будет передано в фильтр. 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.

Условие можно удалить с помощью кнопки ×.

- С помощью кнопки **Добавить группу** добавляются группы условий. Оператор **И** можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

  Группу условий можно удалить с помощью кнопки ×.

- 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 с помощью кнопки ×.

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 в кодировке Unicode.

3. В поле **Предел событий** укажите количество событий, которое должно быть получено, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `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. Значение по умолчанию: `60`.

5. В разделе **Группирующие поля** с помощью кнопки **Добавить поле** выберите поля, по которым будут определяться однотипные события. Вы можете выбрать следующие служебные поля: SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID. Идентификаторы активов добавляются после нормализации события, поэтому по ним можно будет агрегировать события. Остальные служебные поля не используются в агрегации. Выбранные события можно удалять 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 удалять с помощью кнопок со значком крестика.

7. В разделе **Поля суммы** с помощью кнопки **Добавить поле** можно выбрать поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалять 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 с помощью кнопки ✕.

Перейдите к следующему шагу мастера установки.

Шаг 6. Обогащение событий

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.

Поступающие события сначала обогащаются данными из источников, которые вы выбираете на этом шаге мастера, а затем выполняется автоматическое обогащение данными об активах. Например, если у вас настроено dns-обогащение и в результате IP-адрес, указанный в событии, обогатился соответствующим DNS-именем актива, то произойдет обогащение события этим активом.

Коллектор получает сведения об активах от Ядра KUMA и обогащает ими события следующим образом:

- Если в поле события с именем (например, `SourceHostName`) содержится FQDN, совпадающий с FQDN актива, коллектор добавляет поле `SourceAssetID` с идентификатором этого актива. Значение поля `SourceAddress` при этом не учитывается.

- Если в поле события с IP-адресом (например, `DestinationAddress`) указан IP-адрес актива, а поле с именем пустое, коллектор добавляет поле `DestinationAssetID` с идентификатором актива, IP-адрес которого совпадает.

- Если в поле события с именем есть значение, которое не совпадает ни с одним FQDN из базы активов, коллектор не проверяет поле с IP-адресом и не добавляет идентификатор актива. Это относится как к случаям, когда в поле `HostName` указан FQDN, который не соответствует ни одному активу, так и к ситуациям, когда в поле `HostName` указано неполное имя (например, только имя хоста без домена).

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 коллектора существующее правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужное правило обогащения.

Правило обогащения добавлено в набор ресурсов для коллектора.

Чтобы создать в наборе ресурсов коллектора правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

4. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - **шаблон**

     Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

- **таблица**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **обогащение активами**

  Этот тип обогащения используется, когда необходимо добавить обогащение событий активами на определенных коллекторах.

Для обогащения событий активами в блоке **Сопоставление** необходимо заполнить таблицу сопоставления полей события KUMA и полей для записи значениий из хеш-таблицы:

1. Нажмите на кнопку **Добавить**.

2. В раскрывающемся списке **Поле KUMA** выберите одно или несколько полей события, значение которого будет сопоставляться со значением из хеш-таблицы и записываться в соответствующее поле в таблице для записи данных актива.

3. В раскрывающемся списке **Поле для записи данных** выберите поле, в которое, в случае соответствия поля события (**Поле KUMA**) и значения из хеш-таблицы, будет записано значение идентификатора актива.

   Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

   Если пользователь выбирает несколько полей, к значениям полей применяется условие **И**. Если пользователь добавляет несколько строк в столбце **Поле KUMA**, к значениям полей применяется условие **ИЛИ**. Проверка начинается с первого поля в списке. Если значение поля совпадает со значением атрибута, проверка прекращается.

   Например, в событие поступают следующие данные:

   ```
   SourceAddress=192.168.x.xx
   SourceHostName=kuma.example.com.
   ```

   В KUMA есть два актива: *company.example.com* (IP-адрес: 192.168.x.xx, FQDN: company.example.com) и *kuma.example.com* (IP-адрес: 192.168.y.yyy, FQDN: kuma.example.com). Сопоставление для них осуществляется следующим образом:

   - Если пользователь указал отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (company.example.com).

   - Если пользователю важнее получить значение параметра `sourceHostname` (kuma.example.com), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.

   - Если пользователь указал `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

   В таблице сопоставления полей должно быть указано хотя бы одно условие сопоставления.

Вы также можете нажать на кнопку **Применить сопоставление по умолчанию**, расположенную над таблицей. В этом случае будут применены значения параметров **Поле KUMA** и **Поле для записи данных**.

Установленные по умолчанию значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных
`DestinationAddress`	`DestinationAssetID`
`DestinationHostName`	`DestinationAssetID`
`DeviceAddress`	`DeviceAssetID`
`DeviceHostName`	`DeviceAssetID`
`SourceAddress`	`SourceAssetID`
`SourceHostName`	`SourceAssetID`

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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.

- **словарь**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['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 применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
    - **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
    - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
    - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
      - **Символы на замену** – последовательность символов, которую требуется заменить.
      - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

- **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.

  Доступные параметры:

  - **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
  - **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.
  - **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Срок жизни кеша** – время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
  - **Кеш отключен** – с помощью этого переключателя можно включить или отключить кеширование. По умолчанию кеширование включено.
  - **Обновление кеша 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 доступен начиная с KUMA 3.4.1. С помощью переключателя можно включить отправку коллектором KUMA рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения cybertrace-http. Этот тип возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.

  При обогащении через cybertrace коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в CyberTrace содержит квадратные скобки, например **[str1**, **str2]**), KUMA обрабатывает его как массив, а не как строку.

  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. Порт CyberTrace по умолчанию 9999.
  - **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. Значение по умолчанию: `1000`.
  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
  - **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000.
  - **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. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- **cybertrace-http**

  Это новый тип потокового обогащения событий в CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять в системах с большим потоком событий. Производительность cybertrace-http превосходит показатели типа cybertrace.

Ограничения:

- Тип обогащения cybertrace-http неприменим для ретроспективного сканирования в KUMA.
- В случае использования типа обогащения cybertrace-http обнаружения киберугроз не сохраняются в истории CyberTrace в окне Detections.

Доступные параметры:

- **Название** (обязательно) – уникальное название правила обогащения. Максимум 128 символов в кодировке Unicode.
- **Тенант** (обязательно) – имя тенанта, в рамках которого вы планируете вести работу с CyberTrace.
- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443.
- **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
- **Ключевые поля** (обязательно) – список полей событий, используемых для обогащения событий данными из CyberTrace.
- **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000. По достижении 1 млн получаемых событий от сервера CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
- **Основная версия CyberTrace** – выбор версии 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**.
- **Отладка** – переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
- **Теги** – теги для поиска ресурса.

- **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 сервиса, использующего 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 установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис 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**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

  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.

- **проверка DLL Hijacking**

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак KUMA использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения KUMA отправляет запрос с информацией из полей события в KSN. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или корреляторе.

> 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** → **Обнаружение атак DLL Hijacking**).

Доступные параметры:

- **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.

- **Максимальный размер кеша** – максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`.

  Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если KUMA отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.

- **Максимальное количество событий в очереди обогащения** – при превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

- **Выполнять повторный запрос** – в ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса. Если этот параметр включен, настройте дополнительные параметры:

  - **Создавать дубликаты событий** – если этот параметр включен, KUMA создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.
    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
    - Превышено значение, указанное в параметре **Количество запросов**.

    Если этот параметр выключен, KUMA продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.
    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
    - Превышено значение, указанное в параметре **Количество запросов**.

  - **Количество запросов** – максимальное количество запросов в KSN. Если за указанное число запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.

  - **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.

  - **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

- **Прокси-сервер** – параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.

- **Сопоставление** – таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и списком соответствующих полей событий KUMA. Список параметров в запросе:

  - **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: OldFileHash.

  - **Путь до файла DLL** – полный путь, включающий имя файла; рекомендованное поле для сопоставления: OldFilePath. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

    Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

    Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

  - **Хеш процесса (md5)** – рекомендованное поле для сопоставления: FileHash.

- **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

  Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

  Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

- **Имя файла DLL** – рекомендованное поле для сопоставления: OldFileName.

- **Имя процесса** – рекомендованное поле для сопоставления: FileName.

- **Подпись процесса** – необязательный параметр; рекомендованное поле для сопоставления: FileID. В этом поле нужно указать поле KUMA, которое передает Organization из Subject подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.

- **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**.

Для каждого параметра укажите в таблице соответствующее ему поле события KUMA.

5. При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.

6. При необходимости в раскрывающемся списке **Теги** выберите теги для правила обогащения.

7. При необходимости в поле **Описание** добавьте описание правила обогащения. Описание правила может содержать до 4000 символов в кодировке Unicode.

8. В блоке **Параметры фильтра** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке **Фильтр** можно выбрать существующий фильтр или создать новый фильтр.

   Добавление условий и группы условий для фильтра

   Чтобы добавить условия и группы условий для фильтра:

   1. При создании правила обогащения убедитесь, что в блоке **Параметра фильтра** выбрано **Конструктор**.

   2. Нажмите на кнопку **Добавить условие** и в последовательно появляющихся раскрывающихся списках выберите значения событий и оператор фильтра.

      Вы можете добавить несколько условий для фильтра.

   3. При необходимости нажмите на кнопку **Добавить группу**, чтобы добавить группу условий для фильтра.

      Вы можете добавить несколько групп условий.

   4. Нажмите на название логического оператора (**И**, **ИЛИ**, **НЕ**). По умолчанию выбрано значение **И**.

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 поле **Сопоставление с учетными записями LDAP** добавьте одно или несколько названий подключений к LDAP-серверу, которые вы создавали в настройках интеграции с LDAP-сервером.

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 сравнивать с атрибутом LDAP.

   - В столбце **LDAP-атрибут**, укажите атрибут, с которым необходимо сравнивать поле события KUMA. Раскрывающийся список содержит часть стандартных атрибутов, по которым может быть выполнено обогащение. Список 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.

        Список ипортируемых атрибутов из AD

        Из Active Directory можно запросить следующие атрибуты учетных записей:

        - `accountExpires`
        - `badPasswordTime`
        - `cn`
        - `company`
        - `department`
        - `displayName`
        - `distinguishedName`
        - `division`
        - `employeeID`
        - `ipaUniqueID`
        - `l`
        - `mail`
        - `mailNickname`
        - `managedObjects`
        - `manager`

- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`
- `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 для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. 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 помещать идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление успешно.

С помощью кнопки **Добавить** в таблицу можно добавить строку, а с помощью кнопки **Удалить** – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

В список ресурсов коллектора добавлено сопоставление для обогащения событий данными, полученными из LDAP.

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров обогащения требуется остановить и запустить сервис снова.

Перейдите к следующему шагу мастера установки.

https://rutube.ru/video/e07d36a0ad26ad29143c4aca8e58c672/

https://rutube.ru/video/ecf1241640406a2c51970e6b8fb45a0b/

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, например, в маршрутизатор событий - в таком случае следует выбрать коннектор internal на шаге Транспорт. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коллектора существующую точку назначения:

1. В шаге мастера установки **Маршрутизация** нажмите **Добавить**.

2. В открывшемся окне **Создание точки назначения** выберите тип точки назначения, которую вы хотите добавить.

3. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Редактирование точки назначения**, параметры выбранного ресурса отображаются в окне. Параметры точки назначения можно открыть для редактирования в новой вкладке браузера с помощью кнопки ↗.

4. Нажмите **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 шаге мастера установки **Маршрутизация** нажмите **Добавить**.

2. В открывшемся окне **Создание точки назначения** задайте следующие параметры:

   a. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. С помощью переключателя **Состояние** вы можете при необходимости включить или выключить сервис.

   c. В раскрывающемся списке **Тип** выберите тип точки назначения. Доступны следующие значения:

      - internal
      - nats-jetstream
      - tcp
      - http
      - diode
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. На вкладке **Дополнительные параметры** укажите значения для параметров настройки. Набор параметров для настройки зависит от типа точки назначения, выбранного на вкладке **Основные параметры**. Более подробная информация о параметрах и значениях доступна по ссылке для каждого типа точки назначения в пункте c. этой инструкции.

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 KUMA создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коллектора отображается в разделе **Ресурсы** → **Коллекторы**. Его можно использовать для создания новых сервисов коллектора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри решения KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коллектора следует установить на сервере, предназначенном для получения событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите **Сохранить и создать сервис**.

   На вкладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

   Например:

   /opt/kaspersky/kuma/kuma collector --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

   > Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

2. Закройте мастер, нажав **Сохранить коллектор**.

Сервис коллектора создан в KUMA. Теперь сервис необходимо установить на сервере, предназначенном для получения событий.

> Если в коллекторе был выбран коннектор типа wmi, wec или etw, потребуется также установить автоматически созданные агенты KUMA.

Установка коллектора в сетевой инфраструктуре KUMA

Коллектор состоит из двух частей: одна часть создается в веб-интерфейсе KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенной для получения событий. В сетевой инфраструктуре устанавливается вторая часть коллектора.

Чтобы установить коллектор:

1. Войдите на сервер, на котором вы хотите установить сервис.

2. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом>
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY`

   Если в результате выполнения команды были выявлены ошибки, проверьте корректность параметров. Например, наличие требуемого уровня доступа, сетевой доступности между сервисом коллектора и Ядром, уникальность выбранного API-порта. После устранения ошибок продолжите установку коллектора.

   Если ошибки не выявлены, а статус коллектора в веб-интерфейсе KUMA изменился на *зеленый*, остановите выполнение команды и перейдите к следующему шагу.

   > Команду можно скопировать на последнем шаге мастера установщика. В команде 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.

3. Выполните команду повторно, добавив ключ `--install`:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://example.com:7210 --id XXXX --api.port YYYY --install`

4. Добавьте порт коллектора KUMA в исключения брандмауэра.

> Для правильной работы решения убедитесь, что компоненты KUMA могут взаимодействовать с другими компонентами и программами 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 веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.

2. Убедитесь, что у установленного вами коллектора зеленый статус.

   Если статус коллектора отличается от зеленого, просмотрите журнал этого сервиса на машине, где он установлен, 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** веб-интерфейса KUMA:*

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в KUMA.

3. Убедитесь, что в разделе **Ресурсы** веб-интерфейса KUMA в раскрывающемся списке **Хранить исходное 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 KUMA Collectors:

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, которые используют в качестве транспорта коннекторы типа WEC, WMI или ETW, 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 сервис 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 nginx-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 – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections – максимальное число соединений, которые одновременно может открыть рабочий процесс.
```

   При большом количестве активных сервисов и пользователей может понадобиться увеличить лимит открытых файлов в параметрах nginx.conf. Например:

```
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections – максимальное число соединений, которые одновременно может открыть рабочий процесс.
```

4. Перезапустите nginx, выполнив команду:

```
systemctl restart nginx
```

5. На сервере источника событий перенаправьте события на nginx-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 KUMA включены перечисленные в таблице ниже предустановленные коллекторы.

Предустановленные коллекторы

Название	Описание
[OOTB] CEF	Собирает события в формате CEF, поступающие по протоколу TCP.
[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 агента

Агент KUMA состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на сервере или устройстве сетевой инфраструктуры.

Создание агента производится в несколько этапов:

1. **Создание набора ресурсов агента в веб-интерфейсе KUMA**
2. **Создание сервиса агента в веб-интерфейсе KUMA**
3. **Установка серверной части агента на устройстве, с которого требуется передавать события**

Агенты KUMA для устройств Windows можно создать следующим образом:

- Создать вручную путем создания набора ресурсов агента и создания сервиса агента в веб-интерфейсе KUMA.
- Создать автоматически при создании коллектора с типом транспорта wmi, wec или etw. Набор ресурсов и сервис таких агентов создаются в мастере установки коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать события. В созданном вручную агенте коннектор с типом etw следует использовать только в одном подключении. Если вы настроите несколько подключений в созданном вручную агенте etw, статус агента etw будет зеленым, но события не будут передаваться и в журнале агента etw будет ошибка.

На одном устройстве может быть установлено несколько агентов, при этом все агенты должны быть одной версии.

Если на устройстве, где вы планируете создать агент, уже есть установленный агент более старой версии, требуется сначала остановить установленный агент (удалить агент с устройства Windows или перезапустить сервис агента для Linux), а затем можно создавать новый агент. При этом если установлены агенты той же версии, что и планируется создать, остановка агентов не требуется.

При создании и запуске агента версии 3.0.1 и более поздних версий требуется принять условия Лицензионного соглашения.

Создание набора ресурсов для агента

Сервис агента в веб-интерфейсе KUMA создается на основе набора ресурсов для агента, в котором объединяются коннекторы и точки назначения. Типом агента считается тип использованного в нем коннектора. Исключением являются агенты с точкой назначения типа diode: такие агенты считаются diode-агентами.

Чтобы создать набор ресурсов для агента в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** нажмите **Создать**.

   Откроется окно создания агента. В левой части окна отображаются вкладки с общими параметрами агента и подключениями. Вкладка **Общие параметры** будет активна.

2. На вкладке **Общие параметры** выполните следующие действия:

   - В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.
   - Если требуется включить логирование операций сервиса, переведите переключатель **Отладка** в активное положение.
   - Если требуется просматривать имена сервисов или адреса хостов, откуда приходит событие, переведите переключатель **Отслеживать маршрут события** в активное положение.

     Переключатель **Отслеживать маршрут события** доступен, если в подключениях указана хотя бы одна точка назначения с типом **internal**. По умолчанию переключатель находится в положении **Выключено**.
   - В поле **Описание** при необходимости добавьте описание сервиса: до 256 символов в кодировке Unicode.

3. Перейдите на вкладку существующего подключения или создайте подключение с помощью кнопки **Добавить** в нижней части панели слева и переключитесь на вкладку созданного подключения, чтобы изменить его параметры.

   По умолчанию для нового агента создается подключение **Подключение №1**. Новому подключению присваивается название по шаблону **Подключение <номер>**.

Вы можете создать несколько подключений для агента. При необходимости вы можете управлять подключениями:

- переименовывать подключения;
- дублировать подключения;
- удалять подключения.

4. При необходимости в поле **Название подключения** переименуйте подключение для более удобной работы с ними, например, чтобы определить, от какого подключения и с какого агента пришли события. Если вы оставите поле пустым, будет использовано название по шаблону **Подключение <номер>**.

   Длина названия может быть от 1 до 128 символов. Название может содержать только буквы и цифры и не может содержать специальные символы. Пробелы в начале и конце строки названия будут удалены. При вставке названия в поле из буфера обмена, если текст содержит перенос строки, абзац или отступ, эти символы будут заменены на пробел. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.

   Если вы включили отслеживание маршрута события, то при просмотре информации о событии в разделе **События** будет отображаться название подключения, от которого пришло это событие.

5. В блоке параметров **Коннектор** добавьте коннектор:

   - Если хотите выбрать существующий коннектор, выберите его в раскрывающемся списке.
   - Если хотите создать новый коннектор, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
     - В поле **Название** укажите имя коннектора. Название должно содержать от 1 до 128 символов в кодировке Unicode.
     - 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
       - nats-jetstream
       - kafka
       - http
       - file
       - ftp
       - nfs
       - wmi
       - wec
       - snmp

- snmp-trap
- etw
- kata/edr
- office365
- dfi
- vmware
- 1c-log
- 1c-xml

При использовании типа коннектора **tcp**, **udp**, **http**, **wec**, **wmi**, **etw** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса устройств, с которых были получены события.

Возможности по изменению уже созданных wec-. wmi- или etw-подключений в агентах, коллекторах и коннекторах ограничены. Тип подключения можно изменить с **wec** на **wmi** или **etw** обратно, однако типы **wec**, **wmi** и **etw** не получится сменить на какой-либо другой тип подключения. При этом при изменении других типов подключений невозможно выбрать типы **wec**, **wmi** и **etw**. Новые подключения можно создавать без ограничения по типам коннекторов.

При добавлении коннектора типа wmi, wec или etw (существующего или нового) для агента параметры **Режим TLS** и **Сжатие** не будут отображаться на агенте, но их значения будут храниться в его конфигурации. Для нового коннектора эти параметры по умолчанию выключены.
Если для существующего коннектора, выбранного из списка, режим TLS включен, вы не сможете скачать файл конфигурации агента. В этом случае, чтобы скачать файл конфигурации, необходимо перейти в ресурс коннектора, который используется на агенте, и отключить режим TLS.

Коннектор добавлен в выбранное подключение набора ресурсов агента. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

6. В блоке параметров **Точки назначения** добавьте точку назначения.

   - Если хотите выбрать существующую точку назначения, выберите ее в раскрывающемся списке.
   - Если хотите создать новую точку назначения, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
     - В поле **Название** укажите имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
     - В раскрывающемся списке **Тип** выберите тип точки назначения и укажите ее параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:
       - **nats-jetstream** – используется для коммуникации через NATS.
       - **tcp** – используется для связи по протоколу TCP.
       - **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.
     - Включите или выключите переключатель **Состояние**, чтобы включить или выключить отправку событий в точку назначения. По умолчанию этот переключатель включен.

     > Дополнительные параметры точки назначения агента (например, сжатие и режим TLS) должны совпадать с дополнительными параметрами точки назначения коллектора, с которым вы хотите связать агент.

   Точек назначения может быть несколько. Их можно добавить с помощью кнопки **Добавить точку назначения** и удалить с помощью кнопки ✕.

7. Повторите шаги 3–5 для каждого подключения агента, которое вы хотите создать.

8. Нажмите **Сохранить**.

   Набор ресурсов для агента создан и отображается в разделе **Ресурсы** → **Агенты**. Теперь можно создать сервис агента в KUMA.

Управление подключениями для агента

Вы можете управлять созданными для агента подключениями: переименовывать, дублировать или удалять их.

Переименование подключения

По умолчанию новому подключению, созданному в наборе ресурсов для агента, присваивается название по шаблону **Подключение <номер>**. Для более удобной работы с подключениями вы можете переименовывать их, например, чтобы определить, от какого подключения и какого агента пришли события.

Чтобы переименовать подключение:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** создайте новый агент или нажмите на существующий агент в таблице.

2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.

3. Перейдите на вкладку подключения, которое вы хотите переименовать.

4. В поле **Название подключения** измените название подключения.

   Длина названия может быть от 1 до 128 символов. Название может содержать только буквы и цифры и не может содержать специальные символы. Пробелы в начале и конце строки названия будут удалены. При вставке названия в поле из буфера обмена, если текст содержит перенос строки, абзац или отступ, эти символы будут заменены на пробел. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.

5. Нажмите **Сохранить**.

Подключение переименовано. Если вы включили отслеживание маршрута события, то при просмотре информации о событии в разделе **События** будет отображаться название подключения, от которого пришло это событие.

Дублирование подключения

Если вы хотите создать подключение для агента на основе существующего подключения, вы можете создать копию подключения с теми же параметрами.

Чтобы дублировать подключение:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** создайте новый агент или нажмите на существующий агент в таблице.

2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.

3. Перейдите на вкладку подключения, которое вы хотите дублировать, и нажмите на кнопку **Дублировать**.

   Для агента будет создано подключение с такими же параметрами, как в исходном подключении. Новое подключение будет создано с одним из следующих названий:

- Если название исходного подключения соответствовало шаблону **Подключение <номер>**, название дублированного подключения также будет соответствовать этому шаблону. Подключению будет присвоен номер <номер>+1 от номера последнего созданного подключения с названием по такому же шаблону.

- Если исходное подключение ранее было переименовано, новое подключение будет создано с таким же названием. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.

  Вы можете изменить название нового подключения в поле **Название подключения** на вкладке этого подключения.

Удаление подключения

Если для агента создано более одного подключения, вы можете удалить подключение.

Чтобы удалить подключение:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** создайте новый агент или нажмите на существующий агент в таблице.

2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.

3. Перейдите на вкладку подключения, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

   Вы не сможете восстановить подключение после удаления, но вы можете восстановить версию агента, в которой ранее было сохранено это подключение, через историю изменений.

Создание сервиса агента в веб-интерфейсе KUMA

Когда набор ресурсов для агента создан, можно перейти к созданию сервиса агента в KUMA.

Чтобы создать сервис агента в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для агента и нажмите **Создать сервис**.

Сервис агента создан в веб-интерфейсе KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы агента необходимо установить на каждом устройстве, с которого вы хотите передавать данные в коллектор. При установке используется идентификатор сервиса.

Автоматически созданные агенты

При создании коллектора с коннекторами типа wec, wmi или etw автоматически создаются агенты для приема событий Windows.

Автоматически созданные агенты имеют ряд особенностей:

- Автоматически созданные агенты могут иметь только одно подключение.

- Автоматически созданные агенты отображаются в разделе **Ресурсы** → **Агенты**, в конце их названия указаны слова `auto created`. Агенты можно просмотреть или удалить.

- Параметры автоматически созданных агентов указываются автоматически на основе параметров коллектора из разделов **Подключение источников** и **Транспорт**. Изменить параметры можно только в коллекторе, для которого был создан агент.

- В качестве описания автоматически созданного агента используется описание коллектора в разделе **Подключение источников**.

- Отладка автоматически созданного агента включается и выключается в разделе коллектора **Подключение источников**.

- При удалении коллектора с автоматически созданным агентом вам будет предложено удалить коллектор вместе с агентом или удалить только коллектор. При удалении только коллектора агент станет доступен для редактирования.

- При удалении автоматически созданных агентов тип коллектора меняется на **http**, а из поля **URL** коллектора удаляется адрес подключения.

- Если хотя бы одно название журнала Windows указано в коннекторе типа wec или wmi с ошибкой, агент не будет получать события из всех перечисленных в коннекторе журналов Windows. При этом статус агента будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.

- Если в коннекторе типа etw имя сессии указано некорректно, указан не тот провайдер в сессии или указан неверный способ, в каком режиме отправлять события (для корректной отправки событий на стороне Windows Server должен быть указан режим Real time или File and Real time), от агента не будут поступать события, в журнале агента на Windows будет зарегистрирована ошибка, а статус агента будет зеленым. При этом попытки получить события каждые 60 сек не будет. Если вы изменяете параметры сессии на стороне Windows, следует перезапустить агент etw и/или сессию, чтобы изменения были применены.

В интерфейсе KUMA автоматически созданные агенты появляются одновременно с созданием коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать сообщение.

Установка агента в сетевой инфраструктуре KUMA

Когда сервис агента создан в KUMA, можно перейти к установке агента на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

На одном устройстве может быть установлено несколько агентов, при этом все агенты должны быть одной версии.

> Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Установка агента KUMA на устройствах Linux

Агент KUMA, установленный на устройствах Linux, останавливается при закрытии терминала или при перезапуске сервера. Если вы не хотите запускать агенты KUMA вручную, мы рекомендуем устанавливать их с помощью программы, которая автоматически запускает программы при перезапуске сервера, например с помощью программы Supervisor. Если вы хотите запускать агенты KUMA автоматически, укажите в конфигурационном файле KUMA параметры автоматического запуска и перезапуска. Подробнее о настройке параметров автоматического запуска и перезапуска см. официальную документацию программ для автоматического запуска программ.

Пример настройки параметров в программе Supervisor

```
[program:agent_<agent_name>] command=sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port>
autostart=true
autorestart=true
```

где:

- <agent_name> - имя агента KUMA.
- <FQDN> - полное доменное имя сервера Ядра KUMA.
- <port> - номер порта Ядра KUMA.

Чтобы установить агент KUMA на устройство Linux:

1. На устройстве Linux, на котором вы хотите установить агент KUMA, создайте директории для конфигурационного файла и агентов KUMA, например:
   - /opt/kaspersky/kuma;
   - /opt/kaspersky/agent.
2. Поместите конфигурационный файл KUMA в созданную для него директорию. Конфигурационный файл KUMA расположен внутри установщика в директории /kuma-ansible-installer/roles/kuma/files.

   > Убедитесь, что файл kuma имеет достаточные права для запуска.

3. Создайте пользователя KUMA выполнив команду:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

4. Предоставьте пользователю KUMA доступ к директории с конфигурационным файлом KUMA, а также ко всем файлам внутри директории, выполнив команду:

```
sudo chown -R kuma:kuma <path>
```

где:

<path> — путь к директории с конфигурационным файлом KUMA.

5. Установите агент KUMA, выполнив команду:

```
sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --wd <path> [--accept-eula]
```

где:

- <FQDN> — полное доменное имя сервера Ядра KUMA.
- <port> — номер порта Ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210).
- <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса. Параметр `--pair.fingerprint` является необязательным.

  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.

  Если вы хотите указать идентификатор отпечатка для обеспечения проверки подлинности CA-сертификата Ядра KUMA, перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**, установите флажок рядом с сервисом Ядра KUMA, в меню (⋮) выберите **Копировать отпечаток сертификата**, затем скопированный идентификатор используйте в команде установки агента. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.
- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса KUMA.
- <path> — путь к директории, где будут размещаться файлы устанавливаемого агента KUMA. Если не указать этот параметр, файлы будут храниться в директории, где расположен файл kuma.

Вы можете установить два агента KUMA на одном устройстве Linux. В этом случае агенты KUMA будут работать параллельно. При установке второго агента KUMA вам нужно указать для него отдельную директорию с помощью параметра `--wd`.

Для запуска агента вам нужно принять Лицензионное соглашение. Вы можете добавить в команду параметр `--accept-eula`, чтобы автоматически принять Лицензионное соглашение во время установки агента KUMA. В этом случае установка не требует интерактивного взаимодействия. Если вы не укажете этот параметр, вам нужно будет принять или отклонить Лицензионное соглашение самостоятельно во время установки агента KUMA.

Примеры установки агента KUMA:

- Установка агента KUMA без автоматического принятия Лицензионного соглашения:

```
sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX
```

- Установка агента KUMA с автоматическим принятием Лицензионного соглашения:

```
sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX --accept-eula
```

Используя параметр `--accept-eula` во время установки агента KUMA, вы подтверждаете, что согласны с условиями Лицензионного соглашения и принимаете их.

6. Если вы выбрали установку KUMA с автоматическим принятием Лицензионного соглашения и хотите ознакомиться текстом лицензии или в процессе установки вам не был автоматически предоставлен текст Лицензионного соглашения, выполните команду:

```
./agent license --show
```

Агент KUMA будет установлен на устройстве Linux.

Вы можете настроить коллектор для приема данных, которые агент KUMA пересылает в KUMA.

Установка агента KUMA на устройствах Windows

Перед установкой агента KUMA на устройстве Windows убедитесь, что учетная запись, под которой будет запускаться агент KUMA, обладает необходимыми правами.

Права для учетной записи при установке агента KUMA любого типа

Администратору сервера необходимо создать на устройстве Windows учетную запись с правом Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Права для учетной записи при установке агента KUMA типа wec

Администратору сервера необходимо создать на устройстве Windows учетную запись с правами Event Log Readers и Log on as a service. Эту учетную запись необходимо использовать для установки и запуска агента.

Если вы планируете получать события из журнала Security на контроллере домена, предоставьте предустановленной в Windows учетной записи Network Service доступ к журналу Security. Для этого на устройстве контроллера домена в командной строке PowerShell выполните команду:

```
wevtutil sl security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
(A;;0x1;;;S-1-5-20)'
```

> Если вы не настроите доступ к журналу Security, но в параметрах коннектора wec добавите журнал Security, то поток событий от агента KUMA поступать не будет.

Если вы планируете получать события не с контроллера домена, достаточно добавить предустановленную в Windows учетную запись Network Service в группу Event Log Readers.

Права для учетной записи при установке агента KUMA типа wmi

Администратору сервера необходимо создать на устройстве Windows учетную запись с правами Event Log Readers и Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Для запуска агента под доменной учетной записью необходимы права Event Log Readers и Log on as a service.

Если вы хотите запустить агент под локальной учетной записью, для запуска потребуются права администратора, а также права Event Log Readers и Log on as a service.

Если вы хотите выполнить удаленный сбор событий (сбор событий с устройств, подключенных к устройству, на котором установлен агент KUMA) и только чтение журналов под доменной учетной записью, будет достаточно права Event Log Readers.

Права для учетной записи при установке агента KUMA типа etw

Администратору сервера необходимо создать на устройстве Windows учетную запись с правом Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Для запуска агента учетная запись должна обладать правами администратора или должна быть добавлена в одну из групп безопасности:

- Domain admins
- Performance Log Users

Установка агента KUMA

Чтобы установить агент KUMA на устройство Windows:

1. Скопируйте файл kuma.exe в папку на устройстве Windows. Для установки рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

   Файл kuma.exe находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   ```
   kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый
   сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)>
   --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под
   которым будет работать агент, включая домен> --install [--accept-eula]
   ```

Для запуска агента вам нужно принять Лицензионное соглашение. Вы можете добавить в команду параметр `--accept-eula`, чтобы автоматически принять Лицензионное соглашение во время установки агента. В этом случае установка не требует интерактивного взаимодействия. Если вы не укажете этот параметр, вам нужно будет принять или отклонить Лицензионное соглашение самостоятельно во время установки агента KUMA.

Примеры:

- Установка агента KUMA без автоматического принятия Лицензионного соглашения:

  ```
  kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install
  ```

- Установка агента KUMA с автоматическим принятием Лицензионного соглашения:

  ```
  kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install --accept-eula
  ```

> Используя параметр `--accept-eula` во время установки агента KUMA, вы подтверждаете, что согласны с условиями Лицензионного соглашения и принимаете их.

> Справочная информация об установщике доступна по команде `kuma help agent`.

4. Если вы запустили установку агента без автоматического принятия Лицензионного соглашения, в процессе установки вам будет предложено ознакомиться с текстом лицензии и у вас будет возможность принять соглашение или отказаться.

5. Если вы выбрали установку с автоматическим принятием Лицензионного соглашения и хотите ознакомиться текстом лицензии или в процессе установки вам не был автоматически предоставлен текст Лицензионного соглашения, выполните следующую команду:

   ```
   kuma.exe license --show
   ```

   Если вы хотите принять Лицензионное соглашение, выполните следующую команду и нажмите `y`:

   ```
   kuma.exe license
   ```

6. Укажите пароль для пользователя, под которым будет работать агент одним из следующих способов:

   - Вручную.

   - Из файла при установке агента.

     Чтобы не вводить пароль вручную, добавьте пароль в файл в формате .TXT и разместите файл в той же директории, что и бинарный файл агента.

     Укажите в команде содержащий пароль файл следующим образом: `< имя файла с паролем >.txt`. Например, `password.txt`.

     ```
     kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < password.txt
     ```

     Все данные из файла password.txt будут перенаправлены в команду в качестве пароля, за исключением символов конца строки (\n\r , \n).

     Путь хранения папки с агентом после установки: C:\ProgramData\Kaspersky Lab\KUMA\agent\${agent_id}.

Если лицензионное соглашение (EULA) не было принято перед установкой агента с флагом `< password.txt`, появится ошибка с сообщением, о том что соглашение не принято.

Варианты принятия EULA:

a. В файле с паролем можно указать признак принятия EULA. Для этого в файле с паролем должны быть две строки: первая с признаком принятия EULA "y", вторая - с паролем. Например:

```
y
<password>
```

Команда установки агента будет выглядеть следующим образом:

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < password.txt
```

В этом случае при установке агента дополнительно принимать EULA не потребуется.

Если ранее, до запуска команды с файлом-паролем, была принята EULA, первая строка в файле будет воспринята как пароль и установка завершится ошибкой `Access denied`.

b. Можно принять EULA и выполнить тихую установку одновременно, применив флаг --accept-eula.

Команда установки агента будет выглядеть следующим образом:

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --accept-eula --install < password.txt
```

При этом важно, чтобы в файле был указан только пароль первой строкой, иначе возникнет ошибка.

Создана папка `C:\ProgramData\Kaspersky Lab\KUMA\agent\<идентификатор агента>`, в нее установлен сервис агента KUMA. Агент пересылает события Windows в KUMA: можно настроить коллектор для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из веб-интерфейса KUMA, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента KUMA с устройств Windows

Чтобы удалить агент KUMA с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

Указанный агент KUMA удален с устройства Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен>
```

Обновление агентов

При обновлении версий KUMA требуется обновить и установленные на удаленных машинах агенты WMI, WEC и ETW.

Чтобы обновить агент, используйте учетную запись с правами администратора и выполните следующие шаги:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** - **Агенты** выберите агент, который вы хотите обновить, и скопируйте его идентификатор.

   Идентификатор понадобится для последующего удаления агента и установки нового агента с тем же идентификатором.

2. В ОС Windows в разделе **Службы** откройте агент и нажмите **Стоп**.

3. В командном интерпретаторе перейдите в папку, где был установлен агент и выполните команду по удалению агента с сервера.

   kuma.exe agent --id <`идентификатор сервиса агента, созданного в KUMA`> --uninstall

4. Поместите в ту же папку новый агент.

5. В командном интерпретаторе перейдите в папку с новым агентом и из этой папки выполните команду установки, используя идентификатор агента из пункта 1.

   kuma agent --core https://<`полное доменное имя сервера ядра KUMA`>:<`порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)`> --id <`идентификатор сервиса агента, созданного в KUMA`> --user <`имя пользователя, под которым будет работать агент, включая домен`> --install

6. При первой установке обновленного агента на устройстве требуется подтверждение лицензии. В процессе установки вам будет предложено ознакомиться с текстом лицензии и у вас будет возможность принять соглашение или отказаться. Если этого не произошло автоматически, вы можете воспользоваться следующей командой, чтобы ознакомиться с текстом лицензии:

   ```
   kuma.exe license --show
   ```

   Если вы хотите принять лицензионное соглашение, выполните команду и нажмите `y`:

   ```
   kuma.exe license
   ```

Агент обновлен.

Передача в KUMA событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в KUMA. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент KUMA с точкой назначения **diode** принимает события и перемещает их в директорию, из которой события заберет диод данных.

   Агент накапливает события в буфере до его переполнения или в течение заданного пользователем срока после последней записи на диск. Затем события записываются в файл во временной директории агента. Файл перемещается в директорию, обрабатываемую диодом данных; в качестве его названия используется хеш-сумма (SHA-256) содержимого файла и время создания файла.

2. Диод данных перемещает файлы из директории изолированного сервера в директорию внешнего сервера.

3. Установленный на внешнем сервере коллектор KUMA с коннектором **diode** считывает и обрабатывает события из файлов той директории, в которой размещает файлы диод данных.

   После считывания из файла всех событий он автоматически удаляется. Перед считыванием событий происходит верификация содержимого файлов по хеш-сумме в названии файла. Если содержимое не проходит верификацию, файл удаляется.

В указанной выше схеме компоненты KUMA отвечают за перемещение событий в определенную директорию внутри изолированного сегмента и за прием событий из определенной директории во внешнем сегменте сети. Перемещение файлов с событиями из директории изолированного сегмента сети в директорию внешнего сегменте сети осуществляет диод данных.

Для каждого источника данных внутри изолированного сегмента сети необходимо создать свой агент и коллектор KUMA, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов KUMA

Настройка компонентов KUMA для передачи данных из изолированных сегментов сети состоит из следующих этапов:

1. Создание сервиса коллектора во внешнем сегменте сети.

   На этом этапе необходимо создать и установить коллектор для получения и обработки файлов, которые диод данных будет перемещать из изолированного сегмента сети. Создать коллектор и все требуемые для него ресурсы можно с помощью мастера установки коллектора.

   На шаге **Транспорт** требуется выбрать или создать коннектор типа **diode**. В коннекторе необходимо указать директорию, в которую диод данных будет перемещать файлы из изолированного сегмента сети.

   Пользователь kuma, под которым работает коллектор, должен иметь права на чтение, запись и удаление в директории, в которую диод данных перемещает данные из изолированного сегмента сети.

2. Создание набора ресурсов агента KUMA.

На этом этапе необходимо создать набор ресурсов агента KUMA, который будет в изолированном сегменте сети получать события и подготавливать их для передачи диоду данных. Набор ресурсов diode-агента имеет следующие особенности:

- Точка назначения в агенте должна иметь тип **diode**. В этом ресурсе необходимо указать директорию, из которой диод данных будет перемещать файлы во внешний сегмент сети.
- Для diode-агента невозможно выбрать коннекторы типа **sql** или **netflow**.
- В коннекторе diode-агента должен быть выключен режим TLS.

3. Скачивание конфигурационного файла агента в виде JSON-файла.

   a. Набор ресурсов агента с точкой назначения типа diode необходимо скачать в виде JSON-файла.

   b. Если в наборе ресурсов агента использовались ресурсы секретов, конфигурационный файл необходимо вручную дополнить данными секретов.

4. Установка сервиса агента KUMA в изолированном сегменте сети.

   На этом этапе необходимо установить агент в изолированном сегменте сети на основе конфигурационного файла агента, созданного на предыдущем этапе. Установка возможна на устройствах Linux и Windows.

Настройка диода данных

Диод данных необходимо настроить следующим образом:

- Данные необходимо передавать атомарно из директории изолированного сервера (куда их помещает агент KUMA) в директорию внешнего сервера (где их считывает коллектор KUMA).
- Переданные файлы необходимо удалять с изолированного сервера.

Сведения о настройке диода данных можно получить в документации используемого в вашей организации диода данных.

Особенности работы

При работе с изолированными сегментами сети не поддерживаются работа с SQL и NetFlow.

При использовании указанной выше схемы невозможно администрирование агента через веб-интерфейс KUMA, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов KUMA такие агенты не отображаются.

Конфигурационный файл diode-агента

Созданный набор ресурсов агента с точкой назначения типа diode можно скачать в виде конфигурационного файла. Этот файл используется при установке агента в изолированном сегменте сети.

Чтобы скачать конфигурационный файл,

В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** выберите нужный набор ресурсов агента с точкой назначения diode и нажмите **Скачать конфигурацию**.

Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Секреты, использованные в наборе ресурсов агента, скачиваются пустыми, их идентификаторы указаны в файле в разделе `secrets`. Для использования файла конфигурации для установки агента в изолированном сегменте сети необходимо вручную дополнить файл конфигурации секретами (например, указать URL и пароли, используемые в коннекторе агента для получения событий).

Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться diode-агент.

Ниже приводится пример конфигурационного файла diode-агента с коннектором типа kafka.

```
{
  "config": {
    "id": "<идентификатор набора ресурсов агента>",
    "name": "<название набора ресурсов агента>",
    "proxyConfigs": [
      {
        "connector": {
          "id": "<идентификатор коннектора. В этом примере приводится коннектор типа kafka, но в diode-агенте можно использовать коннекторы и других типов. Если коннектор создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
          "name": "<название коннектора>",
          "kind": "kafka",
          "connections": [
            {
              "kind": "kafka",
              "urls": [
                "localhost:9093"
              ],
              "host": "",
              "port": "",
              "secretID": "<идентификатор секрета>",
              "clusterID": "",
              "tlsMode": "",
              "proxy": null,
              "rps": 0,
              "maxConns": 0,
              "urlPolicy": "",
              "version": "",
              "identityColumn": "",
              "identitySeed": "",
              "pollInterval": 0,
              "query": "",
              "stateID": "",
              "certificateSecretID": "",
              "authMode": "pfx",
              "secretTemplateKind": "",
              "certSecretTemplateKind": ""
            }
          ],
          "topic": "<название топика kafka>",
          "groupID": "<идентификатор группы kafka>",
          "delimiter": "",
          "bufferSize": 0,
          "characterEncoding": "",
          "query": "",
          "pollInterval": 0,
          "workers": 0,
          "compression": "",
          "debug": false,
          "logs": [],
          "defaultSecretID": "",
          "snmpParameters": [
            {
              "name": "",
              "oid": "",
              "key": ""
            }
          ],
          "remoteLogs": null,
          "defaultSecretTemplateKind": ""
        },
        "destinations": [
          {
            "id": "<идентификатор точки назначения. Если точка назначения создана непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
            "name": "<название точки назначения>",
            "kind": "diode",
            "connection": {
              "kind": "file",
              "urls": [
                "<путь к директории, в которую точка назначения должна помещать события для передачи из изолированного сегмента сети диодом данных>",
                "<путь к временной директории, в которую помещаются события для подготовки к передаче диодом данных>"
              ],
              "host": "",
              "port": "",
              "secretID": "",
              "clusterID": "",
              "tlsMode": "",
```

```
                "proxy": null,
                "rps": 0,
                "maxConns": 0,
                "urlPolicy": "",
                "version": "",
                "identityColumn": "",
                "identitySeed": "",
                "pollInterval": 0,
                "query": "",
                "stateID": "",
                "certificateSecretID": "",
                "authMode": "",
                "secretTemplateKind": "",
                "certSecretTemplateKind": ""
              },
              "topic": "",
              "bufferSize": 0,
              "flushInterval": 0,
              "diskBufferDisabled": false,
              "diskBufferSizeLimit": 0,
              "healthCheckPath": "",
              "healthCheckTimeout": 0,
              "healthCheckDisabled": false,
              "timeout": 0,
              "workers": 0,
              "delimiter": "",
              "debug": false,
              "disabled": false,
              "compression": "",
              "filter": null,
              "path": ""
            }
          ]
        }
      ],
      "workers": 0,
      "debug": false
    },
    "secrets": {
      "<идентификатор секрета>": {
        "pfx": "<зашифрованный pfx-ключ>",
        "pfxPassword": "<пароль к зашифрованному pfx-ключу. Вместо действительного пароля из KUMA экспортируется значение changeit. В файле конфигурации необходимо вручную указать содержимое секретов>"
      }
    },
    "tenantID": "<идентификатор тенанта>"
}
```


Описание полей секретов

Поля секрета

Название поля	Тип	Описание
`user`	строка	Имя пользователя
`password`	строка	Пароль
`token`	строка	Токен
`urls`	массив строк	Список URL
`publicKey`	строка	Публичный ключ (используется в PKI)
`privateKey`	строка	Приватный ключ (используется в PKI)
`pfx`	строка, содержащая base64-закодированное содержимое pfx	Содержимое pfx-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`
`pfxPassword`	строка	Пароль от pfx

`securityLevel`	строка	Используется в snmp3. Возможные значения: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`
`community`	строка	Используется в snmp1
`authProtocol`	строка	Используется в snmp3. Возможные значения: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
`privacyProtocol`	строка	Используется в snmp3. Возможные значения: `DES`, `AES`
`privacyPassword`	строка	Используется в snmp3
`certificate`	строка, содержащая base64-закодированное содержимое pem	Содержимое pem-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`

Установка Linux-агента в изолированном сегменте сети

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Linux:

1. Поместите на Linux-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя KUMA.

   - Исполняемый файл /opt/kaspersky/kuma/kuma (файл `kuma` можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/).

2. Выполните следующую команду:

   ```
   sudo ./agent agent --cfg <config_path> --wd <directory_path> --install
   ```

   где:

   - <config_path> — путь к конфигурационному файлу агента.
   - <directory_path> — путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл `kuma`.

   Сервис агента установлен и запущен на сервере в изолированном сегменте сети. Он получает события и передает их диоду данных для отправки во внешний сегмент сети.

Установка Windows-агента в изолированном сегменте сети

Перед установкой агента KUMA на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Windows:

1. Поместите на Window-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя, под которым будет работать агент.

   - Исполняемый файл kuma.exe. Файл можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   ```
   kuma.exe agent --cfg <путь к конфигурационному файлу агента> --user <имя пользователя, под которым будет работать агент, включая домен> --install
   ```

   Справочная информация об установщике доступна по команде:

   ```
   kuma.exe help agent
   ```

4. Введите пароль для пользователя, под которым будет работать агент.

   Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент перемещает события в папку для обработки диодом данных.

   При установке агента конфигурационный файл агента перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента, указанный в конфигурационном файле>. Файл kuma.exe перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA.

   При установке агента его конфигурационный файл не должен находиться в директории, в которую устанавливается агент.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев.

Удаление агента KUMA с устройств Windows

Чтобы удалить агент KUMA с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

Указанный агент KUMA удален с устройства Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma.exe agent --cfg <путь к конфигурационному файлу агента>
```

Передача в KUMA событий с машин Windows

Для передачи событий с машин Windows в KUMA используется связка агента и коллектора KUMA. Передача данных организована следующим образом:

1. Установленный на машине агент KUMA получает события Windows:

   - с помощью коннектора WEC: агент получает события, поступающие на хост по подписке (subscription), и журналы сервера.

   - с помощью коннектора WMI: агент подключается к удаленным серверам, указанным в конфигурации, и получает события.

   - с помощью коннектора ETW: агент использует для подключения к DNS-серверу имя сессии и провайдера, указанные в параметрах коннектора, и получает события.

2. Агент без предварительной обработки передает события коллектору KUMA, указанному в точке назначения.

   Можно настроить агент таким образом, чтобы разные журналы отправлялись в разные коллекторы.

3. Коллектор принимает события от агента, выполняет полный цикл обработки события и отправляет обработанные события в точку назначения.

Получение событий с агента WEC рекомендуется при использовании централизованного получения событий с хостов Windows с помощью технологии Windows Event Forwarding (WEF). Агент необходимо установить на сервер, который выполняет сбор событий, он будет выполнять роль Windows Event Collector (WEC). Мы не рекомендуем устанавливать агенты KUMA на каждый конечный хост, с которого планируется получать события.

Процесс настройки получения событий с использованием агента WEC подробно описан в приложении Настройка получения событий с устройств Windows с помощью Агента KUMA (WEC).

Подробнее о технологии Windows Event Forwarding см. в официальной документации Microsoft.

Получение событий с помощью агента WMI рекомендуется использовать в следующих случаях:

- Если отсутствует возможность использовать технологию WEF для реализации централизованного сбора событий, одновременно с этим запрещена установка стороннего ПО на сервере-источнике событий (например, агент KUMA).
- Если необходимо выполнить сбор событий с небольшого количества хостов - не более 500 хостов для одного агента KUMA.

Агент ETW используется только для получения событий из журналов Windows DNS-серверов.

Для подключения журналов Windows в качестве источника событий рекомендуется использовать мастер **Подключить источник**. При использовании мастера в процессе создания коллектора с коннекторами типами WEC и WMI автоматически создаются агенты для приема событий Windows. Также ресурсы, необходимые для сбора событий Windows, можно создать вручную.

Создание и установка агента и коллектора для получения событий Windows происходит в несколько этапов:

1. **Создание набора ресурсов агента.**

   Коннектор агента:

   При создании агента на вкладке **Подключение** необходимо создать или выбрать коннектор типа WEC, WMI или ETW.

   Если хотя бы одно название журнала Windows указано в коннекторе типа WEC или WMI с ошибкой, или недоступен сервер WMI, агент будет получать события из всех перечисленных в коннекторе журналов Windows, кроме проблемного. При этом статус агента будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.

   Точка назначения агента:

   Тип точки назначения агента зависит от используемого вами способа передачи данных: nats-jetstream, tcp, http, diode, kafka, file.

   В качестве разделителя в точке назначения необходимо использовать значение `\0`.

   Дополнительные параметры точки назначения агента (например, разделитель, сжатие и режим TLS) должны совпадать с дополнительными параметрами коннектора коллектора, с которым вы хотите связать агент.

2. **Создание сервиса агента в веб-интерфейсе KUMA.**

3. **Установка агента KUMA на машине Windows, с которой вы хотите получать события Windows.**

   Перед установкой убедитесь, что компоненты системы имеют доступ к сети и откройте необходимые сетевые порты:

   - Порт 7210, протокол TCP: от сервера с коллекторами к Ядру.
   - Порт 7210, протокол TCP: от сервера агента к Ядру.
   - Порт, настроенный при создании коннектора в поле **URL**: от сервера агента к серверу с коллектором.

4. **Создание и установка коллектора KUMA.**

   При создании набора ресурсов коллектора на шаге **Транспорт** необходимо создать или выбрать существующий коннектор, с помощью которого коллектор будет получать события от агента. Тип коннектора должен совпадать с типом точки назначения агента.

   Дополнительные параметры коннектора, такие как разделитель, сжатие и режим TLS, должны совпадать с дополнительными параметрами точки назначения агента, с которой вы хотите связать агент.

Импорт файла со списком серверов для агентов WMI

Вы можете импортировать файл в формате .TSV со списком источников событий для агентов WMI, чтобы не заполнять вручную параметры **Сервер**, **Домен** и **Тип журналов** для агента WMI каждого сервера, когда таких серверов много. В таком файле вы можете подготовить список серверов, к которым будет подключаться агент WMI, и список журналов, которые вы хотите получать от указанных серверов.

Требования к файлу со списком серверов для агентов WMI

Допустимый формат файла: TSV.

Если вы поменяете рекомендуемый формат на **All files** и загрузите файл, не соответствующий требуемому формату (например, вместо TSV загружен файл JSON, XML или в другом формате), парсинг такого файла может быть выполнен некорректно.

Максимальное количество строк в файле с параметрами хостов: 500.

Следующие поля являются обязательными для заполнения:

- **Сервер** – имя хоста, от которого агент будет получать журналы. Допустимый формат: имя хоста или IP-адрес. Допустимые значения: IPv4, IPv6, имя хоста.
- **Домен** – идентификатор хоста, по которому будет выполняться обращение к хосту по сети. Допустимый формат: полное доменное имя или IP-адрес. Допустимые значения: IPv4, IPv6, FQDN.
- **Тип журналов** – список журналов и/или подписок Windows, которые будет получать агент. Допустимый формат: массив строк. Например, вы можете указать значение Application, ForwardedEvents или Security. Если в файле указано значение, ранее отсутствовавшее в списке журналов, должны быть созданы пользовательский журнал или подписка, которые также появятся в списке доступных к обработке с помощью Windows-агента.

  Допустимо указать значение журнала, которое имеет максимальную длину – 1024 символа. Должно быть указано не менее одного журнала или подписки.

После импорта и заполнения всех полей удаленных хостов при сохранении параметров выполняется проверка. Если в полях допущены ошибки, параметры не сохранятся, а допущенные ошибки будут выделены. Вы можете вручную внести необходимые правки в полях и сохранить параметры.

Чтобы импортировать файл со списком источников:

1. В разделе KUMA **Ресурсы** → **Агенты** создайте агент WMI или откройте параметры агента WMI для редактирования.
2. В открывшемся окне на вкладке **Подключение №** в блоке параметров **Коннектор** укажите название коннектора, в раскрывающемся списке **Тип** выберите **wmi** и нажмите на кнопку **Импорт TSV**.
3. В открывшемся окне выберите подготовленный файл со списком источников в формате .TSV.

   KUMA выполняет парсинг файла и в блоке параметров **Удаленные хосты** заполняет данными обязательные поля **Сервер**, **Домен**, **Тип журналов**.

4. При необходимости в раскрывающемся списке **Секрет** выберите секрет с типом **Credentials** либо создайте секрет с типом **Credentials**.

   При импорте списка хостов из файла, в раскрывающемся списке **Секрет** остается значение **По умолчанию** и агент будет применять учетные данные по умолчанию при обращении к серверу для получения журналов.

5. Если вы хотите отменить импорт данных из файла, нажмите **Отмена**. Если вы хотите убрать некоторые строки с данными, импортированными из файла, в интерфейсе выделите необходимые для удаления строки и нажмите **Удалить**.

6. Сохраните параметры, выполнив одно из следующих действий:

   - Для созданного агента нажмите **Создать**. Сервис будет создан в веб-интерфейсе KUMA.

   - Для действующего агента, открытого для редактирования, нажмите **Сохранить**.

7. Примените сохраненные параметры, выполнив одно из следующих действий:

   - Для созданного агента установите сервис агента в сетевой инфраструктуре KUMA.

   - Для действующего сервиса агента, открытого для редактирования, перезапустите сервис агента.

Файл со списком серверов для агентов WMI будет импортирован.

AI-сервисы

В этом разделе представлена информация об AI-сервисах, с которыми работает KUMA.

AI рейтинг и AI-статус активов

Сервис **AI-рейтинг и AI-статус активов** доступен для установки при условии, что 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 **Рейтинг AI** и **Статус AI**. Если лицензионный ключ удалить, поля **Рейтинг AI** и **Статус AI** будут скрыты из карточки актива. Если лицензионный ключ снова добавить, значения полей **Рейтинг AI** и **Статус AI** снова будут отображаться.

Рейтинг – это число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля **Статус AI**: **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 **Рейтинг AI** и **Статус AI**. Также вы можете настроить проактивную категоризацию активов по полям **Рейтинг AI** и **Статус AI** 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 и удаление 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. Сохраните файл сертификата Ядра KUMA в директории установщика roles/mlservice/files.

6. Перейдите в директорию с файлами сервиса и из этой директории выполните команду:

   ```
   ./install <путь к inventory.yaml>
   ```

7. 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.

8. 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-рейтинг 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. Установите переключатель **Состояние** в активное положение. По умолчанию переключатель находится в неактивном положении.

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 веб-интерфейсе KUMA 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.

Параметр	Описание
`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
`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.

Проанализировать с помощью KIRA

В KUMA есть возможность проанализировать с помощью Kaspersky Investigation & Response Assistant (далее KIRA) команду, на которую сработало корреляционное правило. Команда записывается в поле события, если нормализация настроена таким образом, чтобы команда попадала в поле события. Вы можете просмотреть команду в карточке события или карточке корреляционного события и нажать **Проанализировать с помощью KIRA** в верхней части карточки события, чтобы отправить запрос в KIRA. KIRA выполнит деобфускацию и покажет результат предыдущего запроса по команде из кеша, если такой запрос был выполнен ранее. Эта функция помогает расследовать алерты и инциденты. Результаты анализа хранятся в кеше в течение 14 дней и доступны для повторного просмотра. Каждый раз при отправке запроса создается событие аудита.

Функция доступна в регионе RU при следующих условиях:

- 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

- При настройке интеграции с KIRA загружен сертификат. Файл сертификата в формате PFX, запакованный в архив <имя заказчика>.ZIP, и пароль к сертификату, можно получить у сотрудников 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.

Настройка интеграции с KIRA

Чтобы настроить интеграцию с KIRA:

1. Получите лицензию с AI-модулем и активируйте функциональность в KUMA.
2. В веб-консоли KUMA перейдите в раздел **Параметры** → **Интеграции** → **AI-сервисы**.
3. В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant**.
4. Включите интеграцию с KIRA, установив переключатель **Статус** в активное положение.

   По умолчанию переключатель выключен.
5. Нажмите **Выбрать файл** и загрузите архив <имя заказчика>.ZIP, в котором содержится сертификат в формате PFX.
6. В поле **Пароль от сертификата** укажите пароль.
7. В раскрывающемся списке **Прокси-сервер** выберите ранее созданный ресурс или создайте новый.
8. В раскрывающемся списке 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.
9. 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.

Выполнение анализа с помощью KIRA

После того как интеграция настроена, можно выполнить анализ команды с помощью KIRA.

Чтобы выполнить анализ:

1. Перейдите в карточку события или корреляционного события и на панели инструментов в карточке события в раскрывающемся списке **Проанализировать с помощью KIRA** выберите поле, значение которого вы хотите проанализировать.

2. В открывшемся окне **Проанализировать с помощью KIRA** отобразится команда для анализа. Доступны следующие возможности:

   - Если команда обфусцирована, деобфускация будет выполнена автоматически без расхода токенов. Если вы хотите проанализировать команду в обфусцированном виде, в раскрывающемся списке **Действия** выберите **Вернуть исходную строку**. При необходимости вы можете деобфусцировать строку снова.

   - Если вы хотите предварительно определить количество токенов, которые будут затрачены на анализ, в раскрывающемся списке **Действия** выберите **Рассчитать размер в токенах**. Количество токенов для анализа = количество токенов на отправку запроса + количество токенов на ответ.

   - Чтобы проанализировать команду, нажмите кнопку **Проанализировать**.

     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 команды выполнен.

Результат анализа доступен в том же окне **Проанализировать с помощью KIRA**: вывод, краткое содержание и развернутый анализ. Также вы можете просмотреть результат в отдельном окне, если нажмете **Посмотреть результат** на всплывающем уведомлении. Откроется отдельное окно **Результат KIRA**, из которого можно **Перейти к событию** по ссылке. После выполнения анализа **Результат** будет отображаться в карточке события на вкладке **Анализ KIRA** и будет доступен для просмотра всем пользователям с доступом к функциональности **Проанализировать с помощью KIRA**.

Также вы можете просмотреть результат анализа в разделе **Диспетчер задач** в свойствах задачи **Запрос в KIRA**. Если вы нажмете на название задачи, в контекстном меню будут доступны следующие действия:

- **Посмотреть результат** – в этом случае любой пользователь с доступом к задачам KIRA может просмотреть результаты выполнения задачи из кэша и токены не будут потрачены.

- **Перезапустить** – в этом случае анализ будет выполнен без учета данных предыдущего анализа, хранящихся в кеше, и токены будут потрачены на выполнение анализа.

Возможные ошибки задачи Проанализировать с помощью KIRA

Возможные ошибки

HTTP-код	Описание
400	Недействительный клиентский сертификат.
404	Ошибка в запросе.
401	Отсутствует информация о сертификате. Обратитесь в техническую поддержку.

403	Суточный лимит токенов исчерпан.
413	Достигнуто максимальное количество токенов для выполнения запроса. Следует уменьшить запрос.
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 используется модуль AI. Модуль AI анализирует параметры запуска и исполнения программ 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. Мы рекомендуем встраивать обогащение этого типа в коррелятор, а не в коллектор. В корреляторе проверка проводится на корреляционном событии, а в коллекторе – на базовом. Так как корреляционных событий намного меньше, чем базовых, запросов для проверки корреляционных событий требуется намного меньше. 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** → **Обнаружение атак DLL Hijacking**). 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 решения 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. Мы рекомендуем использовать нормализатор [OOTB] KEDR Telemetry, импортированный из репозитория.

4. В разделе **Корреляция** создайте правило корреляции типа simple или типа standard. В правиле корреляции укажите поля, которые вы указали при добавлении обогащения. 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.

5. 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.

6. Если вы хотите настроить решение 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`

Обнаружение атак DLL Hijacking настроено. Если вы создали правило корреляции, то при получении заключений **Подозрительная** или **Вредоносная** будет создаваться алерт.

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 решения 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 решение 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`

Обнаружение атак DLL Hijacking настроено. Если вы создали правило корреляции, то при получении заключений **Подозрительная** или **Вредоносная** будет создаваться алерт.

Сервис Метрики

Для мониторинга работы сервисов KUMA и потока событий от источников в KUMA выполняется сбор и хранение большого количества данных. Для сбора, хранения и анализа данных используется сервис Метрики.

Метрики все время доступны на сервисах KUMA. Сервис Метрики собирает значения этих метрик с интервалом 15с. Если сервис KUMA недоступен, будут потеряны изменения кратные `<время простоя>` / `<интервал сбора>`.

Начиная с версии KUMA 4.2 при первичной установке KUMA сервис Метрики устанавливается на хосте, указанном в секции `kuma_metrics` в файле инвентаря. Также вы можете установить сервис Метрики на произвольном хосте. В любой конфигурации KUMA сервис Метрики должен быть только один. При обновлении с версии KUMA 4.0 до версии 4.2 в файле инвентаря в секции `kuma_metrics` необходимо указать хост, на котором запущен активный сервис Метрики. При запуске обновления выполняется проверка и если сервис Метрики на этом хосте не найден, вернется ошибка и обновление прервется.

В отказоустойчивой конфигурации KUMA сервис Метрики обращается к доступному Ядру KUMA напрямую, без участия балансировщика.

Если ранее работал один сервис Метрики и после его удаления был установлен новый сервис, исторические данные не удаляются автоматически. Данные сервиса Метрики остаются в директории /opt/kaspersky/kuma/metrics/<`идентификатор бывшего экземпляра сервиса Метрики`>/data. Для переноса данных сервиса Метрики на другой хост скопируйте их до первого запуска нового сервиса, сохранив права доступа. При необходимости замените существующий каталог data на перенесённый, предварительно остановив сервис.

Установка сервиса Метрики на хосте

Установка сервиса Метрики выполняется с помощью установщика expand.sh и файла инвентаря expand.inventory.yml.

Чтобы установить сервис Метрики на хосте:

1. Убедитесь, что на целевых машинах соблюдены аппаратные и программные требования, а также требования к установке.

2. На контрольной машине перейдите в директорию с распакованным установщиком KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

3. Скопируйте шаблон expand.inventory.yml.template и создайте файл инвентаря с именем expand.inventory.yml:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

4. Отредактируйте параметры файла инвентаря expand.inventory.yml и в секции `kuma_metrics` укажите хост, на котором вы хотите установить сервис Метрики.

5. На контрольной машине с доступом root из папки с распакованным установщиком выполните следующую команду:

   ./expand.sh expand.inventory.yml

   В результате выполнения команды на хосте, указанном в секции `kuma_metrics`, появятся файлы для создания и установки сервиса Метрики.

6. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы** в раскрывающемся списке **Добавить** выберите **Добавить сервис Метрики**.

7. В открывшемся окне **Добавить сервис Метрики** укажите название сервиса в поле **Имя сервиса Метрики**.

8. Нажмите **Добавить**.

   Окно Добавить сервис Метрики свернется, в правом верхнем углу появится уведомление "Сервис Метрики добавлен" и будет выполнен переход в раздел **Активные сервисы**. Сервис Метрики добавлен в список сервисов и находится в красном статусе.

9. В разделе Активные сервисы установите флажок рядом с сервисом Метрики и на панели инструментов или в меню (⋮) выберите **Копировать идентификатор**.

10. Установите сервис Метрики на хосте, указанном в файле инвентаря expand.inventory.yml. Для этого в консоли командной строки выполните следующую команду:

    ```
    sudo /opt/kaspersky/kuma/kuma metrics --core https://< FQDN сервера Ядра KUMA >:< порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210) > --id < идентификатор сервиса, скопированный из веб-интерфейса KUMA > --api.port < порт, используемый для связи с устанавливаемым компонентом > --install
    ```

```
Пример: sudo /opt/kaspersky/kuma/kuma metrics --core https://kuma.example.com:7210 --
id XXXX --api.port YYYY --install
```

11. Если вы хотите перенести исторические данные прежнего сервиса Метрики, скопируйте директорию data со старого хоста на новый, сохранив все атрибуты файлов (владельца, группу, права доступа, временные метки):

    ```
    sudo mv /opt/kaspersky/kuma/metrics/<идентификатор прежнего сервиса Метрики>/data
    /opt/kaspersky/kuma/metrics/<идентификатор нового сервиса Метрики>/data
    ```

    После копирования убедитесь, что директория data и содержащиеся в ней файлы принадлежат пользователю и группе, под которыми работает сервис Метрики (по умолчанию kuma:kuma):

    sudo chown -R kuma:kuma /opt/kaspersky/kuma/metrics/<`идентификатор нового сервиса Метрики`>/data

    sudo chmod -R 750 /opt/kaspersky/kuma/metrics/<`идентификатор нового сервиса Метрики`>/data

12. Выполните запуск сервиса Метрики с помощью следующей команды:

    ```
    sudo systemctl start metrics.service
    ```

Сервис Метрики установлен и запущен.

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. **Настройка коллектора KUMA для получения событий Auditd**
2. **Настройка сервера источника событий**

   Вы можете настроить сервер источника событий с помощью сервиса rsyslog или syslog-ng.
3. **Проверка поступления событий Auditd в коллектор KUMA**

   Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка коллектора KUMA для получения событий Auditd

На шаге **Транспорт** выберите тип коннектора **TCP** или **UDP** и переведите переключатель **Auditd** в активное положение.

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 с помощью сервиса rsyslog

Для передачи событий от сервера в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере источнике событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующую команду:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. Откройте файл сервиса audit.service /etc/audit/auditd.conf и измените значения следующих параметров:

   ```
   name_format=NONE
   log_format=ENRICHED
   ```

   Параметр `log_format` определяет формат записей, создаваемых сервисом auditd, и должен иметь значение `ENRICHED`, чтобы в событиях сохранялась информация о пользователях.

   После изменения параметров перезапустите сервис auditd с помощью команды:

   ```
   sudo systemctl restart auditd.service
   ```

3. В папке /etc/rsyslog.d создайте файл audit.conf со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $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>
     Например:
     *.* @@192.1.3.4:5858
     ```

   - Для отправки событий по протоколу UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/audit/audit.log
     ```

```
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
template(name="AuditFormat" type="string" string="<%PRI%>%TIMESTAMP:::date-rfc3339%
%HOSTNAME% %syslogtag% %msg%\n")
*.* @<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
Например:
*.* @192.1.3.4:5858;AuditFormat
```

4. Сохраните изменения в файле audit.conf.

5. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор KUMA.

Настройка сервера источника событий с помощью сервиса syslog-ng

Для передачи событий от сервера в коллектор KUMA используется сервис syslog-ng.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере-источнике событий установлен сервис syslog-ng, выполнив следующую команду:

```
systemctl status syslog-ng.service
```

Если сервис syslog-ng не установлен на сервере, установите его, выполнив команду в соответствии с вашей системой управления пакетами:

- Для APT (Debian, Ubuntu):

```
apt install syslog-ng
```

- Для YUM (CentOS 7, RHEL):

```
yum install syslog-ng
```

- Для DNF (Fedora, CentOS 8):

```
dnf install syslog-ng
```

- Для Zypper (openSUSE):

```
zypper install syslog-ng
```

- Для Pacman (Arch Linux):

```
pacman -S syslog-ng
```

- Для Snap (если доступно):

```
snap install syslog-ng
```

2. После установки запустите сервис syslog-ng:

```
systemctl enable syslog-ng.service
systemctl start syslog-ng.service
```

3. Откройте файл параметров /etc/audit/auditd.conf сервиса audit.service и измените значение параметра `name_format`, присвоив этому параметру значение `NONE`:

   `name_format=NONE`

4. После изменения параметра перезапустите сервис auditd с помощью команды:

```
sudo systemctl restart auditd.service
```

5. В папке /etc/syslog-ng создайте файл audit.conf со следующим содержанием в зависимости от используемого протокола:

- Для отправки событий по протоколу TCP:

```
source s_audit_log {
    file("/var/log/audit/audit.log"
      persist-name("s_audit_log_for_siem")
      follow-freq(1)
      program-override("auditd:")
      flags(no-parse));
  };
  log {
    source(s_audit_log);
    destination(d_audit_log);
  };
```

```
# Форматирование сообщений
```

```
  template AuditFormat {
    template("<${PRI}>${ISODATE} ${HOST} ${MSG}\n");
```

```
};
```

```
# Передача журналов аудита на указанный адрес коллектора KUMA
```

```
destination d_audit_log {
  tcp("<IP-адрес коллектора KUMA>" port(<порт коллектора KUMA>) persist-
  name("collector-audit") template(AuditFormat));
};
```

- Для отправки событий по протоколу UDP:

```
source s_audit_log {
  file("/var/log/audit/audit.log"
    persist-name("s_audit_log_for_siem")
    follow-freq(1)
    program-override("auditd:")
    flags(no-parse));
};
log {
  source(s_audit_log);
  destination(d_audit_log);
};
```

```
# Форматирование сообщений
```

```
template AuditFormat {
  template("<${PRI}>${ISODATE} ${HOST} ${MSG}\n");
};
```

```
# Передача журналов аудита на указанный адрес коллектора KUMA
```

```
destination d_audit_log {
  udp("<IP-адрес коллектора KUMA>" port(<порт коллектора KUMA>) persist-
  name("collector-audit") template(AuditFormat));
};
```

6. Сохраните изменения в файле audit.conf.

7. Добавьте в конфигурационный файл /etc/syslog-ng/syslog-ng.conf следующую строку:

```
@include " audit.conf "
```

8. Перезапустите сервис syslog-ng, выполнив следующую команду:

```
systemctl restart syslog-ng.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 веб-интерфейсе KUMA убедитесь, что номер порта и тип коннектора совпадают с портом и протоколом, указанными в параметрах передачи событий Kaspersky Anti Targeted Attack Platform в KUMA.

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. Создание коллектора KUMA
3. Установка коллектора KUMA в сетевой инфраструктуре
4. 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 веб-интерфейсе 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. Укажите следующие параметры:

   a. Установите флажки **Журнал активности** и **Обнаружения**.

   b. В поле **Хост/IP** введите IP-адрес или имя хоста 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 хоста** укажите идентификатор хоста 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 на кнопку **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 веб-интерфейсе KUMA для событий Kaspersky Anti Targeted Attack Platform.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c настроек 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.

Настройка передачи событий Kaspersky Security Center в SIEM-систему KUMA

KUMA позволяет получать и передавать события от Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA.

Настройка передачи и получения событий Kaspersky Security Center состоит из следующих этапов:

1. Настройка передачи событий Kaspersky Security Center.
2. Настройка коллектора KUMA.
3. Установка коллектора KUMA в сетевой инфраструктуре.
4. Проверка поступления событий Kaspersky Security Center в коллектор KUMA.

   Вы можете проверить, что экспорт событий из Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA выполнен правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Чтобы отобразить события Kaspersky Security Center в таблице, введите следующее поисковое выражение:

```
SELECT * FROM `events` WHERE DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

Настройка передачи событий Kaspersky Security Center в формате CEF

Kaspersky Security Center позволяет настроить параметры экспорта событий в SIEM-систему в формате CEF.

Функция экспорта событий Kaspersky Security Center в SIEM-системы в формате CEF доступна при наличии лицензии Kaspersky Endpoint Security для бизнеса Расширенный или выше.

Чтобы настроить передачу событий от Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA:

1. В дереве консоли Kaspersky Security Center выберите узел **Сервер администрирования**.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите **Настроить экспорт в SIEM-систему**.

   Откроется окно **Свойства: События**. По умолчанию откроется раздел **Экспорт событий**.
4. В разделе **Экспорт событий** установите флажок **Автоматически экспортировать события в базу SIEM-системы**.
5. В раскрывающемся списке **SIEM-система** выберите **ArcSight (CEF-формат)**.
6. Укажите адрес сервера SIEM-системы KUMA и порт для подключения к серверу в соответствующих полях. В качестве протокола выберите **TCP/IP**.

   Вы можете нажать на кнопку **Экспортировать архив** и указать дату, начиная с которой уже созданные события KUMA будут экспортироваться в базу SIEM-системы. По умолчанию Kaspersky Security Center экспортирует события с текущей даты.
7. Нажмите на кнопку **OK**.

В результате Сервер администрирования Kaspersky Security Center будет автоматически экспортировать все события в SIEM-систему KUMA.

Настройка коллектора KUMA для сбора событий Kaspersky Security Center

После завершения настройки экспорта событий от Сервера администрирования Kaspersky Security Center в формате CEF вам нужно настроить коллектор в веб-интерфейсе KUMA.

Чтобы настроить коллектор KUMA для событий Kaspersky Security Center:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коллекторы**.
2. В списке коллекторов найдите коллектор с нормализатором **[OOTB] KSC** и нажмите на него, чтобы открыть для редактирования.
3. На шаге **Транспорт** в поле **URL** укажите порт, по которому коллектор будет получать события Kaspersky Security Center.

   Порт должен совпадать с портом сервера SIEM-системы KUMA.
4. На шаге **Парсинг событий** проверьте, что выбран нормализатор **[OOTB] KSC**.
5. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.
   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.
6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
7. Скопируйте появившуюся команду для установки коллектора KUMA.

Установка коллектора KUMA для сбора событий Kaspersky Security Center

После завершения настройки коллектора для сбора событий Kaspersky Security Center в формате CEF требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий Kaspersky Security Center из MS SQL

KUMA позволяет получать информацию о событиях Kaspersky Security Center из базы данных MS SQL (далее MS SQL).

Перед настройкой убедитесь, что вы создали коллектор KUMA для событий Kaspersky Security Center из MS SQL.

При создании коллектора в веб-интерфейсе KUMA на шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**.

Для получения событий Kaspersky Security Center из БД MS SQL на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**

Настройка получения событий состоит из следующих этапов:

1. Создание учетной записи в MS SQL.
2. Настройка службы SQL Server Browser.
3. Создание секрета.
4. Настройка коннектора.
5. Установка коллектора в сетевой инфраструктуре.
6. Проверка поступления событий из MS SQL в коллектор KUMA.

   Вы можете проверить, что настройка поступления событий из MS SQL выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Создание учетной записи в MS SQL

Для получения событий Kaspersky Security Center из MS SQL требуется учетная запись, которая имеет права, необходимые для подключения и работы с базой данных.

Чтобы создать учетную запись для работы с MS SQL:

1. Войдите на сервер с установленной MS SQL для Kaspersky Security Center.
2. С помощью **SQL Server Management Studio** подключитесь к MS SQL под учетной записью с правами администратора.
3. В панели Object Explorer раскройте раздел **Security**.
4. Нажмите правой кнопкой мыши на папку **Logins** и в контекстном меню выберите **New Login**.

   Откроется окно **Login - New**.

5. На вкладке **General** нажмите на кнопку **Search** рядом с полем **Login name**.
   Откроется окно **Select User or Group**.
6. В поле **Enter the object name to select (examples)** укажите имя объекта и нажмите **OK**.
   Окно **Select User or Group** закроется.
7. В окне **Login - New** на вкладке **General** выберите опцию **Windows authentication**.
8. В поле **Default database** выберите БД Kaspersky Security Center.
   По умолчанию имя БД Kaspersky Security Center: KAV.
9. На вкладке **User Mapping** настройте права для учетной записи:
   a. В разделе **Users mapped to this login** выберите БД Kaspersky Security Center.
   b. В разделе **Database role membership for** установите флажки возле прав **db_datareader** и **public**.
10. На вкладке **Status** настройте права для подключения учетной записи к базе данных:
    - В разделе **Permission to connect to database engine** выберите **Grant**.
    - В разделе **Login** выберите **Enabled**.
11. Нажмите **OK**.
    Окно **Login - New** закроется.

Чтобы проверить права учетной записи:

1. Запустите **SQL Server Management Studio** под созданной учетной записью.
2. Перейдите в любую таблицу MS SQL и сделайте выборку по таблице.

Настройка службы SQL Server Browser

После создания учетной записи в MS SQL требуется настроить службу SQL Server Browser.

Чтобы настроить службу SQL Server Browser:

1. Откройте **SQL Server Configuration Manager**.
2. В левой панели выберите **SQL Server Services**.
   Откроется список служб.
3. Откройте свойства службы **SQL Server Browser** одним из следующих способов:
   - Дважды нажмите на название службы **SQL Server Browser**.
   - Нажмите правой кнопкой мыши на название службы **SQL Server Browser** и в контекстном меню выберите **Properties**.
4. В открывшемся окне **SQL Server Browser Properties** выберите вкладку **Service**.

5. В поле **Start Mode** выберите **Automatic**.

6. Выберите вкладку **Log On** и нажмите на кнопку **Start**.

   Автоматический запуск службы **SQL Server Browser** включен.

7. Включите и настройте протокол **TCP/IP**, выполнив следующие действия:

   a. В левой панели раскройте раздел **SQL Server Network Configuration** и выберите подраздел **Protocols for <Имя SQL-сервера>**.

   b. Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстом меню выберите **Enable**.

   c. В появившемся окне **Warning** нажмите **OK**.

   d. Откройте свойства протокола **TCP/IP** одним из следующих способов:

      - Дважды нажмите на протокол **TCP/IP**.

      - Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстном меню выберите **Properties**.

   e. Выберите вкладку **IP Addresses**, а затем в разделе **IPALL** в поле **TCP Port** укажите порт 1433.

   f. Нажмите на кнопку **Apply**, чтобы сохранить внесенные изменения.

   g. Нажмите на кнопку **OK**, чтобы закрыть окно.

8. Перезагрузите службу **SQL Server (<Имя SQL-сервера>)**, выполнив следующие действия:

   a. В левой панели выберите **SQL Server Services**.

   b. В списке служб справа нажмите правой кнопкой мыши на службу **SQL Server (<Имя SQL-сервера>)** и в контекстном меню выберите **Restart**.

9. В **Брандмауэре защитника Windows в режиме повышенной безопасности** разрешите на сервере входящие подключения по порту TCP 1433.

Создание секрета в KUMA

После создания и настройки учетной записи в MS SQL требуется добавить секрет в веб-интерфейсе KUMA. Этот ресурс используется для хранения учетных данных для подключения к MS SQL.

Чтобы создать секрет в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **urls**.

   d. В поле **URL** укажите строку вида:
   `sqlserver://[<domain>%5C]<username>:<password>@<server>:1433/<database_name>`

   где:

   - `domain` – имя домена.
   - `%5C` – разделитель домена и пользователя. Представляет собой знак "\" в URL-формате.
   - `username` – имя созданной учетной записи MS SQL.
   - `password` – пароль созданной учетной записи MS SQL.
   - `server` – имя или IP-адрес сервера с базой данных MS SQL, установленной для Kaspersky Security Center.
   - `database_name` – имя БД Kaspersky Security Center. Имя по умолчанию: KAV.

   Пример:
   `sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV`

   Если в пароле учетной записи БД MS SQL используются специальные символы (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), переведите их в формат URL.

4. Нажмите **Сохранить**.

Из соображений безопасности после сохранения секрета строка, указанная в поле URL, скрывается.

Настройка коннектора

Для подключения KUMA к БД MS SQL требуется настроить коннектор.

Чтобы настроить коннектор:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.

2. В списке коннекторов справа найдите коннектор **[OOTB] KSC SQL** и откройте его для редактирования.

   Если коннектор недоступен для редактирования, скопируйте его и откройте для редактирования копию коннектора.

Если коннектор **[OOTB] KSC SQL** отсутствует, обратитесь к системному администратору.

3. На вкладке **Основные параметры** в раскрывающихся списках **URL** выберите секрет, созданный для подключения к БД MS SQL.

4. Нажмите **Сохранить**.

Настройка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Kaspersky Security Center из MS SQL.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе KUMA на шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**.

Для получения событий Kaspersky Security Center из MS SQL на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**

Установка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL

После завершения настройки коллектора для получения событий Kaspersky Security Center из MS SQL требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий с устройств Windows с помощью Агента KUMA (WEC)

KUMA позволяет получать информацию о событиях с устройств Windows с помощью Агента KUMA типа WEC.

Настройка получения событий состоит из следующих этапов:

1. Настройка политик получения событий с устройств Windows.

2. Настройка централизованного получения событий с помощью службы Windows Event Collector.

3. Предоставление прав для просмотра событий.

4. Предоставление прав входа в качестве службы.

5. Настройка коллектора KUMA.

6. Установка коллектора KUMA.

7. Передача в KUMA событий с устройств Windows.

[▷]

https://rutube.ru/video/805cf2c4e1e804a4cc3aa4f1f92d6407/

Настройка аудита событий с устройств Windows

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве, так и на всех устройствах в домене.

В этом разделе описывается настройка аудита на отдельном устройстве, а также настройка аудита с помощью групповой политики домена.

Настройка политики аудита на устройстве Windows

Чтобы настроить политики аудита на устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.

4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

- Аудит входа в систему
- Аудит изменения политики
- Аудит системных событий
- Аудит событий входа в систему
- Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Помимо настройки политики аудита на отдельном устройстве, вы также можете настроить аудит с помощью групповой политики домена.

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.
2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.
3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Если вы хотите получать журналы Windows с большого количества серверов или если установка агентов KUMA на контроллеры домена не допускается, рекомендуется настроить перенаправление журналов Windows на отдельные серверы с настроенной службой Windows Event Collector.

Настройка политики аудита на сервере или рабочей станции завершена.

Настройка централизованного получения событий с устройств Windows с помощью службы Windows Event Collector

Служба Windows Event Collector позволяет централизованно получать данные о событиях на серверах и рабочих станциях под управлением ОС Windows. С помощью службы Windows Event Collector вы можете подписаться на события, которые регистрируются на удаленных устройствах.

Вы можете настроить следующие типы подписок на события:

- **Source-initiated subscriptions**. Удаленные устройства отправляют данные о событиях на сервер Windows Event Collector, адрес которого указывается в групповой политике. Подробнее о процедуре настройки подписки см. в разделе Настройка передачи данных с сервера источника событий.

- **Collector-initiated subscriptions**. Сервер Windows Event Collector подключается к удаленным устройствам и самостоятельно забирает события из локальных журналов. Подробнее о процедуре настройки подписки см. в разделе Настройка сервиса получения событий Windows.

Настройка передачи данных с сервера источника событий

Вы можете получать информацию о событиях на серверах и рабочих станциях, настроив передачу данных с удаленных устройств на сервер Windows Event Collector.

Предварительная подготовка

1. Проверьте, что служба Windows Remote Management настроена на сервере источника событий, выполнив следующую команду в консоли PowerShell:

   ```
   winrm get winrm/config
   ```

   Если служба Windows Remote Management не настроена, инициализируйте ее, выполнив следующую команду:

   ```
   winrm quickconfig
   ```

2. Если сервер источника событий является контроллером домена, откройте доступ по сети к журналам Windows, выполнив следующую команду в консоли PowerShell, запущенной от имени администратора:

   ```
   wevtutil set-log security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)'
   ```

   Проверьте наличие доступа, выполнив следующую команду:

   ```
   wevtutil get-log security
   ```

Настройка брандмауэра сервера источника событий

Для того чтобы сервер Windows Event Collector мог получать записи журналов Windows, требуется открыть порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `wf.msc` и нажмите **OK**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.

3. Перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего пользователя**.

4. На шаге **Тип правила** выберите **Для порта**.

5. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP**. В поле **Определенные локальные порты** укажите номера портов:

   - `5985` (для доступа по HTTP)

   - `5986` (для доступа по HTTPS)

   Вы можете указать один из портов или оба.

6. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

7. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

8. На шаге **Имя** укажите имя правила для нового входящего подключения и нажмите **Готово**.

Настройка передачи данных с сервера источника событий завершена.

> Сервер Windows Event Collector должен обладать правами для чтения журналов Windows на сервере источника событий. Права могут быть предоставлены как учетной записи сервера Windows Event Collector, так и специальной пользовательской учетной записи. Подробнее о предоставлении прав см. в разделе Предоставление прав пользователю для просмотра журнала событий Windows.

Настройка сервиса получения событий Windows

Сервер Windows Event Collector может самостоятельно подключаться к устройствам и забирать данные о событиях любого уровня важности.

Чтобы настроить получение данных о событиях сервером Windows Event Collector:

1. На сервере-источнике событий откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `services.msc` и нажмите **OK**.

   Откроется окно **Службы**.

3. В списке служб найдите службу **Сборщик событий Windows** и запустите ее.

4. Откройте оснастку **Просмотр событий**, выполнив следующие действия:

   a. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

   b. В открывшемся окне введите запрос `eventvwr` и нажмите **OK**.

5. Перейдите в раздел **Подписки** и в панели **Действия** нажмите **Создать подписку**.

6. В открывшемся окне **Свойства подписки** задайте имя и описание подписки, а также следующие параметры:

   a. В поле **Конечный журнал** выберите из списка **Перенаправленные события**.

   b. В разделе **Тип подписки и исходные компьютеры** нажмите на кнопку **Выбрать компьютеры**.

   c. В открывшемся окне **Компьютеры** нажмите на кнопку **Добавить доменный компьютер**.

      Откроется окно **Выбор: "Компьютер"**.

   d. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена устройств, с которых вы хотите получать информацию о событиях. Нажмите **OK**.

   e. В окне **Компьютеры** проверьте список устройств, с которых сервер Windows Event Collector будет забирать данные о событиях и нажмите **OK**.

   f. В окне **Свойства подписки** в поле **Собираемые события** нажмите на кнопку **Выбрать события**.

   g. В открывшемся окне **Фильтр запроса** укажите, как часто и какие данные о событиях на устройствах вы хотите получать.

   h. При необходимости в поле **<Все коды событий>** перечислите коды событий, информацию о которых вы хотите или не хотите получать. Нажмите **OK**.

7. Если вы хотите использовать специальную учетную запись для просмотра данных о событиях, выполните следующие действия:

   a. В окне **Свойства подписки** нажмите на кнопку **Дополнительно**.

   b. В открывшемся окне **Дополнительные параметры подписки** в настройках учетной записи пользователя выберите **Определенный пользователь**.

   c. Нажмите на кнопку **Пользователь и пароль** и задайте учетные данные выбранного пользователя.

Настройка сервиса получения событий завершена.

Чтобы проверить, что настройка выполнена правильно и данные о событиях поступают на сервер Windows Event Collector,

в оснастке **Просмотр событий** перейдите в раздел **Просмотр событий (Локальный)** → **Журналы Windows** → **Перенаправленные события**.

Предоставление прав для просмотра событий Windows

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

   Откроется окно **Управление компьютером**.

3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.

4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите **OK**.

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.

2. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.

4. Перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.

5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите **OK**.

Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите **OK**.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите **OK**.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Настройка коллектора KUMA для получения событий с устройств Windows

После завершения настройки политики аудита на устройствах, а также создания подписок на события и предоставления всех необходимых прав, требуется создать коллектор в веб-интерфейсе KUMA для событий с устройств Windows.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

Для получения событий от устройств Windows в мастере установки коллектора KUMA укажите следующие параметры коллектора:

1. На шаге **Транспорт** укажите следующие параметры:

   a. В поле **Коннектор** выберите **Создать**.

   b. В поле **Тип** выберите **http**.

   c. В поле **Разделитель** выберите **\0**.

2. На вкладке **Дополнительные параметры** в поле **Режим TLS** выберите **С верификацией**.

3. На шаге **Парсинг событий** нажмите на кнопку **Добавить парсинг событий**.

4. В открывшемся окне **Основной парсинг событий** в поле **Нормализатор** выберите **[OOTB] Microsoft Products** и нажмите **OK**.

5. На шаге **Маршрутизация** добавьте следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.

   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их

6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора KUMA.

Установка коллектора KUMA для получения событий с устройств Windows

После завершения настройки коллектора для получения событий Windows требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка передачи в KUMA событий с устройств Windows с помощью Агента KUMA (WEC)

Чтобы завершить настройку передачи данных, требуется создать агент KUMA типа WEC, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Подробнее о создании и установке агента KUMA типа WEC на устройства Windows см. в разделе Передача в KUMA событий с устройств Windows.

Настройка получения событий с устройств Windows с помощью Агента KUMA (WMI)

KUMA позволяет получать информацию о событиях с устройств Windows с помощью Агента KUMA типа WMI.

Настройка получения событий состоит из следующих этапов:

1. Настройка параметров аудита для работы с KUMA.
2. Настройка передачи данных с сервера источника событий.
3. Предоставление прав для просмотра событий.
4. Предоставление прав входа в качестве службы.
5. Создание коллектора KUMA.

   Для получения событий от устройств Windows в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Microsoft Products**.
6. Установка коллектора KUMA.
7. Передача в KUMA событий с устройств Windows.

   Чтобы завершить настройку передачи данных, требуется создать агент KUMA типа WMI, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

[▷]

https://rutube.ru/video/805cf2c4e1e804a4cc3aa4f1f92d6407/

Настройка параметров аудита для работы с KUMA

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве с помощью локальной политики, так и на всех устройствах в домене с помощью групповой политики.

В этом разделе описывается настройка аудита на отдельном устройстве, а также настройка аудита с помощью групповой политики домена.

Настройка аудита с помощью локальной политики

Чтобы настроить аудит с помощью локальной политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.

4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Помимо настройки аудита на отдельном устройстве вы также можете настроить аудит с помощью групповой политики домена.

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.

4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

- Аудит входа в систему
- Аудит изменения политики
- Аудит системных событий
- Аудит событий входа в систему
- Аудит управления учетными записями

Настройка политики аудита на сервере или рабочей станции завершена.

Настройка передачи данных с сервера источника событий

Предварительная подготовка

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.
2. В открывшемся окне введите запрос `services.msc` и нажмите **OK**.

   Откроется окно **Службы**.
3. В списке служб найдите следующие службы:
   - Удаленный вызов процедур
   - Сопоставитель конечных точек RPC
4. Убедитесь, что в графе **Состояние** у этих служб отображается статус **Выполняется**.

Настройка брандмауэра сервера источника событий

Сервер Windows Management Instrumentation может получать записи журналов Windows, если открыты порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.
2. В открывшемся окне введите запрос `wf.msc` и нажмите **OK**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.
3. В окне **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего подключения**.

4. В **Мастере создания правила для нового входящего подключения** на шаге **Тип правила** выберите **Для порта**.

5. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP**. В поле **Определенные локальные порты** укажите номера портов:

   - `135`
   - `445`
   - `49152-65535`

6. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

7. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

8. На шаге **Имя** укажите имя правила для нового входящего подключения и нажмите **Готово**.

Настройка передачи данных с сервера источника событий завершена.

Предоставление прав для просмотра событий Windows

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

   Откроется окно **Управление компьютером**.

3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.

4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите **OK**.

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.

2. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.

4. В окне **Active Directory Пользователи и Компьютеры** перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.

5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В окне **Выбор пользователя, компьютера или группы** в поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите **OK**.

Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. В окне **Локальная политика безопасности** перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить пользователя или группу**.

   Откроется окно **Выбор "Пользователи или "Группы"**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите **OK**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **`Win`**+**`R`**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить пользователя или группу**.

   Откроется окно **Выбор "Пользователи или "Группы"**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите **OK**.

Настройка получения событий DNS-сервера с помощью агента ETW

Коннектор Event Tracing for Windows (далее также коннектор ETW) – это механизм ведения журнала событий, создаваемых приложениями и драйверами на DNS-сервере. Вы можете использовать коннектор ETW для устранения ошибок при разработке, а также для поиска вредоносной активности.

Использование коннектора ETW оказывает незначительное влияние на производительность DNS-сервера. Например, DNS-сервер, который работает на современном оборудовании и получает до 100 000 запросов в секунду (англ. queries per second, QPS), может испытывать снижение производительности на 5% при использовании коннектора ETW. Если DNS-сервер получает до 50 000 запросов в секунду, снижение производительности не наблюдается. Мы рекомендуем следить за производительностью DNS-сервера при использовании коннектора ETW вне зависимости от количества запросов в секунду.

> По умолчанию вы можете использовать коннектор ETW на операционной системе Windows Server, начиная с версии Windows Server 2016. Коннектор ETW также поддерживается версией Windows Server 2012 R2, если установлено исправление для ведения журнала событий и аудита изменений. Исправление доступно на сайте службы технической поддержки Microsoft.

Коннектор ETW состоит из следующих компонентов:

- *Поставщики* или *провайдеры* (англ. providers) – элементы системы, которые генерируют события и отправляют их коннектору ETW. Например, поставщиками могут быть ядра Windows или драйвера устройств. При работе с кодом разработчикам нужно указать, какие события поставщики отправляют коннектору ETW. Событием может быть выполнение важной с точки зрения разработчика функции, например функции, которая открывает доступ к Security Account Manager (SAM).

- *Потребители* (англ. consumers) – программные системы, получают от коннектора ETW события, сгенерированные поставщиками, после чего используют эти события. Например, потребителем может быть KUMA.

- *Контроллеры* (англ. controllers) – программы, которые управляют взаимодействием между поставщиками и потребителями. Например, контроллерами могут быть утилиты Logman или Wevtutil. Поставщики регистрируются в контроллере для отправки событий потребителям. Контроллер может включить или выключить поставщика. Если поставщик выключен, он не генерирует события.

Для установки связи между поставщиками и потребителями контроллеры используют сессии трассировки. Сессии трассировки также используются для фильтрации данных по указанным параметрам, так как потребителям могут требоваться разные события.

Настройка получения событий DNS-сервера с помощью коннектора ETW состоит из следующих этапов:

1. Настройка на стороне Windows.

2. Создание коллектора KUMA.

При создании коллектора KUMA выполните следующие действия:

a. На 2-м шаге мастера установки коллектора выполните следующие действия:

   1. В раскрывающемся списке **Тип** выберите тип коннектора **tcp**. Вы также можете указать тип коннектора **http** и другие типы коннектора с верификацией для защищенной отправки.

   2. В поле **URL** введите FQDN и номер порта, на котором коллектор KUMA будет ожидать соединения от агента KUMA. Вы можете указать номер любого из незанятых портов.

   3. В поле **Разделитель** введите `\n`.

b. На 3-м шаге мастера установки коллектора в раскрывающемся списке **Нормализатор** выберите нормализатор. Мы рекомендуем выбрать предустановленный расширенный нормализатор для событий Windows **[OOTB] Microsoft DNS ETW logs json**.

c. На 7-м шаге мастера установки коллектора добавьте точку назначения с типом **Хранилище** для хранения событий. Если вы планируете использовать корреляцию по событиям, вам также нужно добавить точку назначения с типом **Коррелятор**.

d. На 8-м шаге мастера установки коллектора нажмите на кнопку **Сохранить и создать сервис**, после чего в нижней части окна скопируйте команду для установки коллектора KUMA на сервере.

3. Установка коллектора KUMA на сервере.

   Выполните следующие действия:

   a. Подключитесь к интерфейсу командной строки KUMA, используя учетную запись пользователя с правами root.

   b. Установите коллектор KUMA, выполнив команду, которую вы скопировали на 8-м шаге мастера установки коллектора.

   c. Если вы хотите добавить порт коллектора KUMA в исключения межсетевого экрана и обновить параметры межсетевого экрана, выполните команды:

      1. `firewall-cmd --add-port=<номер порта коллектора>/tcp –permanent`

      2. `firewall-cmd --reload`

   Коллектор KUMA будет установлен, и статус сервиса коллектора KUMA изменится на зеленый в веб-интерфейсе KUMA.

4. Создание агента KUMA.

   При создании агента KUMA выполните следующие действия:

   a. Выберите вкладку **Подключение 1**.

   b. В блоке параметров **Коннектор** раскрывающемся списке **Коннектор** выберите **Создать** и укажите следующие параметры:

      1. В раскрывающемся списке **Тип** выберите тип коннектора **etw**.

      2. В поле **Имя сессии** введите имя поставщика, которое вы указали при настройке получения событий DNS-сервера с помощью коннектора ETW на стороне Windows.

c. В блоке параметров **Точки назначения** в раскрывающемся списке **Точка назначения** выберите **Создать** и укажите следующие параметры:

1. В раскрывающемся списке **Тип** выберите тип точки назначения **tcp**.

2. В поле **URL** введите FQDN и номер порта, на котором коллектор KUMA будет ожидать соединения от агента KUMA. Введенное значение должно совпадать со значением, которое вы указали на 2-м шаге мастера установки коллектора.

d. Выберите вкладку **Дополнительные параметры** и в поле **Размер дискового буфера** введите `1073741824`.

5. Создание сервиса агента KUMA.

   Вам нужно скопировать идентификатор созданного сервиса агента KUMA. Для этого нажмите на правую кнопку мыши рядом с сервисом агента KUMA и в контекстном меню выберите пункт **Копировать идентификатор**.

6. Создание учетной записи для агента KUMA.

   Создайте доменную или локальную учетную запись Windows для запуска агента KUMA и обеспечения доступа к чтению аналитического журнала. Вам нужно добавить созданную учетную запись в группу пользователей **Пользователи журналов производительности** (англ. **Performance Log Users group**), а также назначить этой учетной записи право **Вход в качестве службы** (англ. **Log on as a service**).

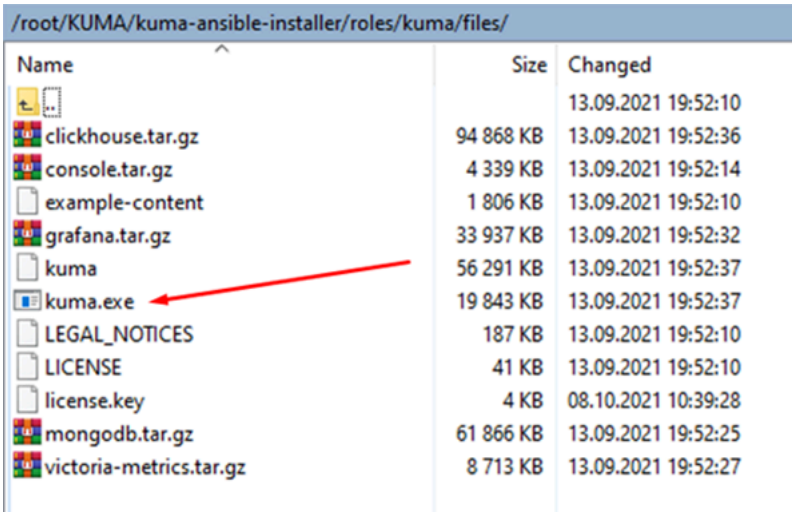
7. Установка агента KUMA на Windows-сервере.

   Вам нужно установить агент KUMA на Windows-сервере, который будет обеспечивать прием событий от поставщика. Для этого выполните следующие действия:

   a. Добавьте FQDN сервера KUMA Core в файл hosts на Windows-сервере, либо на DNS-сервер.

   b. Создайте директорию C:\Users\<имя пользователя>\Desktop\KUMA на Windows-сервере.

   c. Скопируйте файл kuma.exe из архива пакетов установки KUMA в директорию C:\Users\<имя пользователя>\Desktop\KUMA.



   d. Запустите командную строку от имени администратора.

   e. Перейдите в директорию C:\Users\<имя пользователя>\Desktop\KUMA и выполните команду:

```
C:\Users\< имя пользователя >\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id < идентификатор сервиса агента KUMA >
```

В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** убедитесь, что сервис агента KUMA был запущен и его статус изменился на зеленый, после чего прервите выполнение команды.

f. Запустите установку агента KUMA одним из следующих способов:

- Если вы хотите запустить установку агента KUMA с использованием доменной учетной записи, выполните команду:

  ```
  C:\Users\< имя пользователя >\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id < идентификатор сервиса агента KUMA > --user < домен >\< имя учетной записи для агента KUMA > --install
  ```

- Если вы хотите запустить установку агента с использованием локальной учетной записи, выполните команду:

  ```
  C:\Users\< имя пользователя >\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id < идентификатор сервиса агента KUMA > --user < имя учетной записи для агента KUMA > --install
  ```

Вам потребуется ввести пароль учетной записи для агента KUMA.

На Windows-сервере будет установлен сервис KUMA Windows Agent <идентификатор сервиса агента KUMA>. Если в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** сервис агента KUMA не запущен и имеет красный статус, вам нужно убедиться в доступности портов 7210, а также порта коллектора Windows по направлению от агента KUMA к коллектору KUMA.

Для удаления сервиса агента KUMA на Windows-сервере выполните команду:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --id < идентификатор сервиса агента KUMA > --uninstall
```

8. Проверка поступления событий DNS-сервера в коллектор KUMA.

   Вы можете проверить, что настройка получения событий DNS-сервера с помощью коннектора ETW выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка на стороне Windows

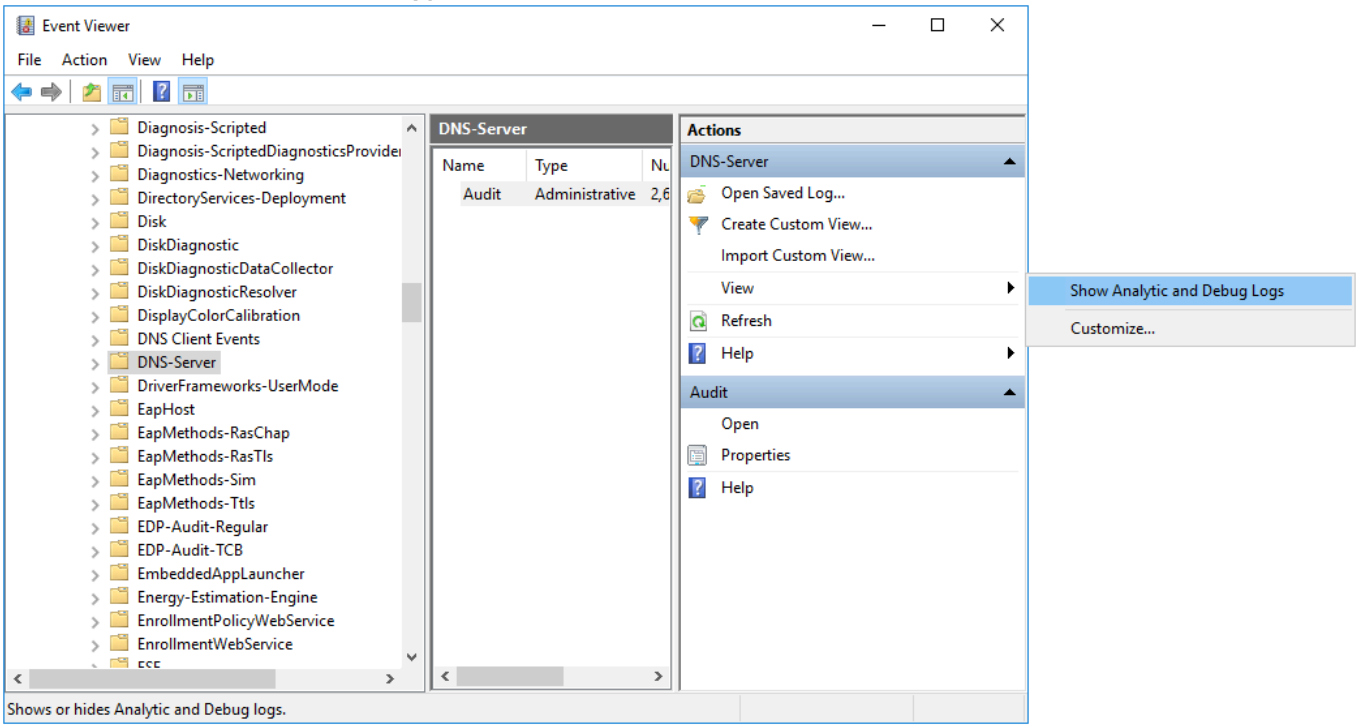
Чтобы настроить получение событий DNS-сервера с помощью коннектора ETW на стороне Windows:

1. Запустите Просмотр событий (англ. Event viewer), выполнив команду:

   ```
   eventvwr.msc
   ```

2. В открывшемся окне перейдите в директорию **Журналы приложений и служб** → **Microsoft** → **Windows** → **DNS-Server**.

3. Откройте контекстное меню директории **DNS-Server** и выберите пункт **Вид** → **Отобразить аналитический и отладочный журналы**.

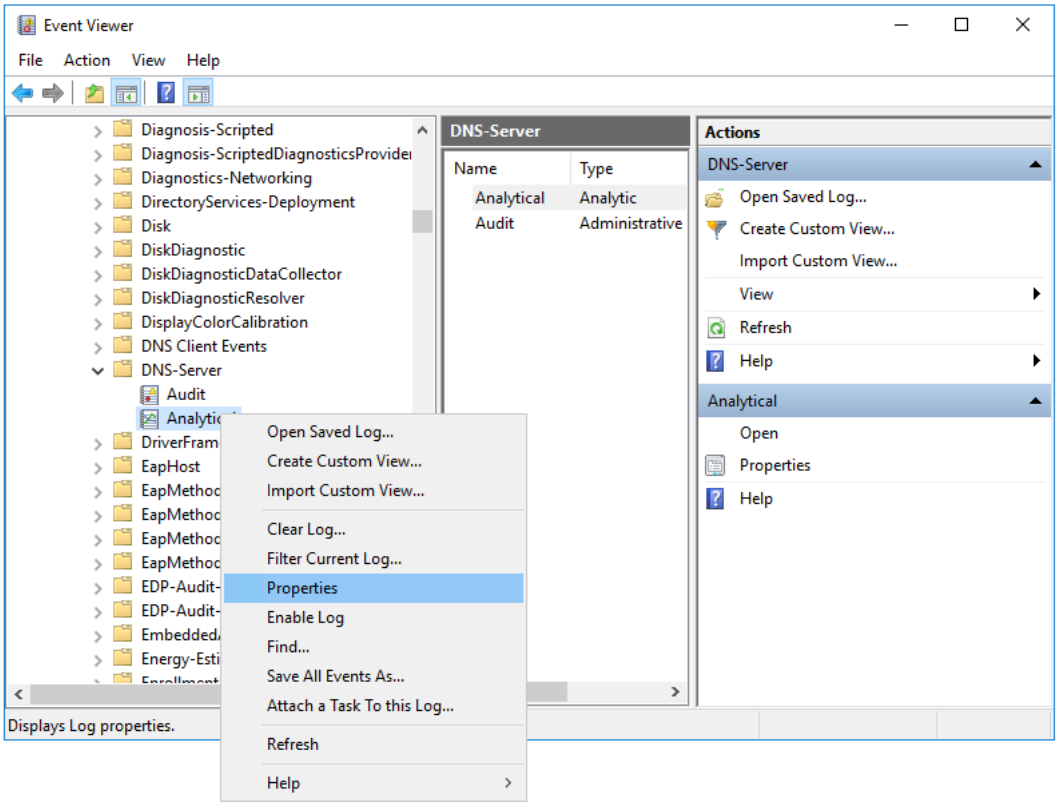


Отображение аналитического и отладочного журнала

Отобразится отладочный журнал **Audit** и аналитический журнал **Analytical**.

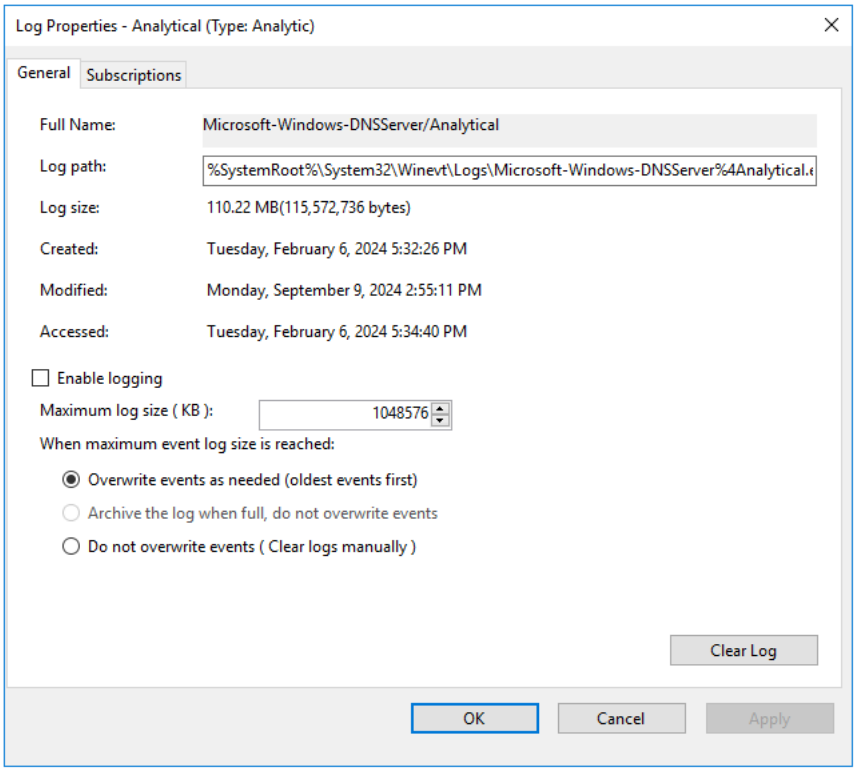
4. Настройте аналитический журнал:

a. Откройте контекстное меню аналитического журнала **Analytical** и выберите пункт **Свойства**.



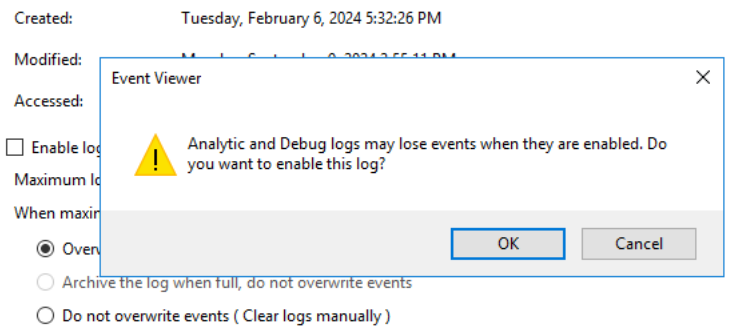
Переход в свойства аналитического журнала Analytical

a. В открывшемся окне убедитесь, что в поле **Макс. размер журнала (КБ)** указано значение `1048576`.



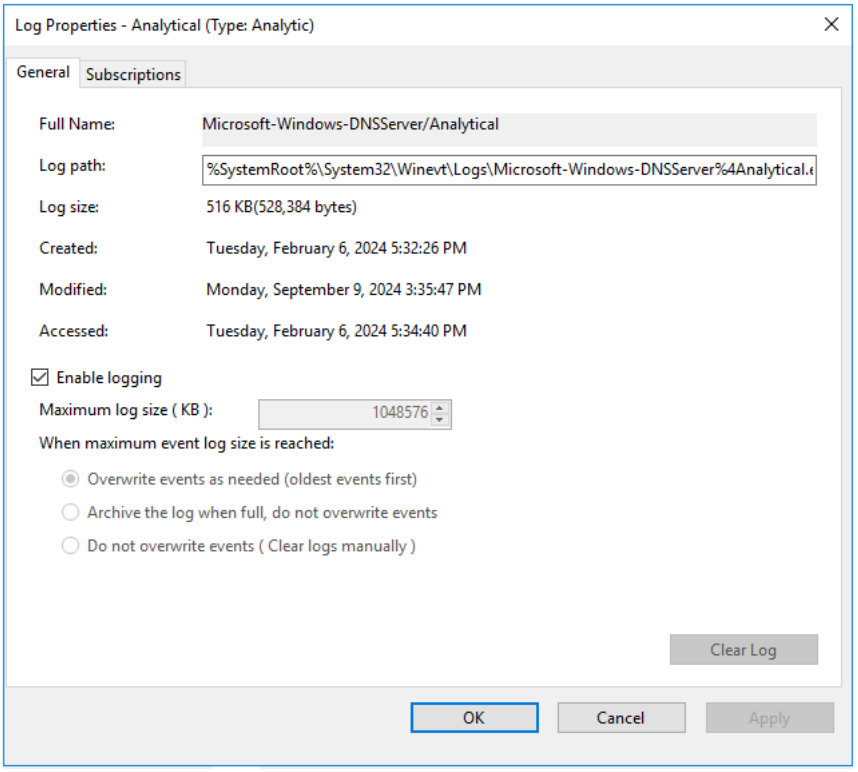
Свойства аналитического журнала Analytical

a. Установите флажок **Включить ведение журнала** и в открывшемся окне подтверждения нажмите на кнопку **OK**.



Окно подтверждения

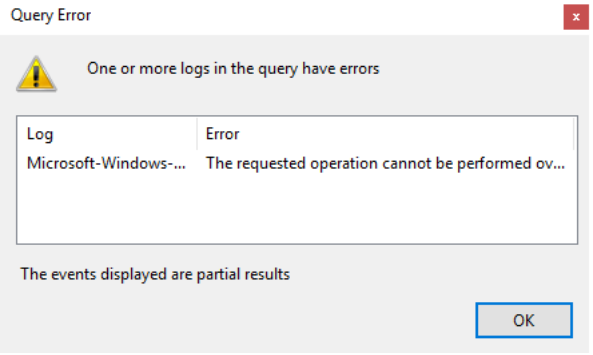
Параметры аналитического журнала должны быть настроены следующим образом:



Проверка корректности параметров аналитического журнала Analytical

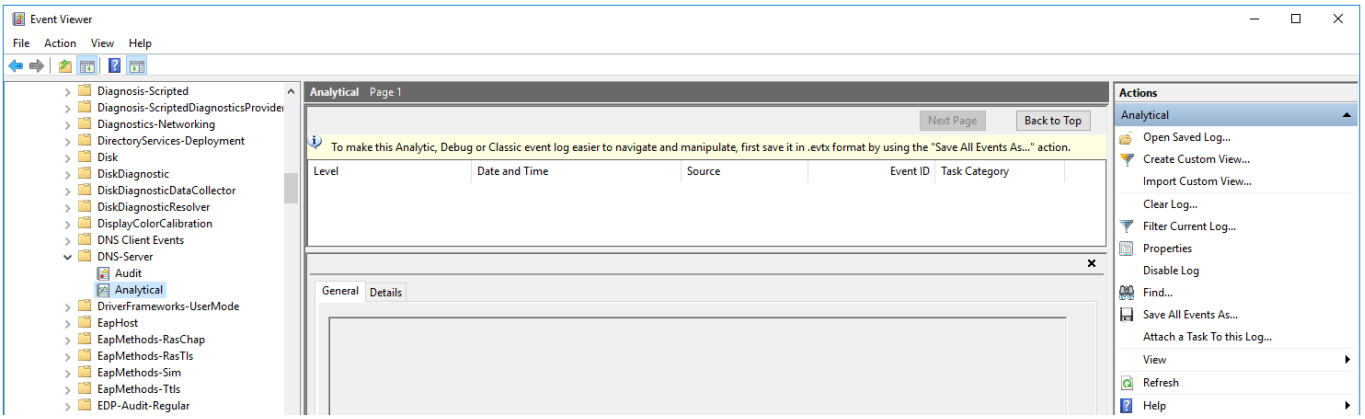
a. Нажмите на кнопку **Применить**, после чего нажмите на кнопку **OK**.

Отобразится окно с ошибкой.



Окно ошибки

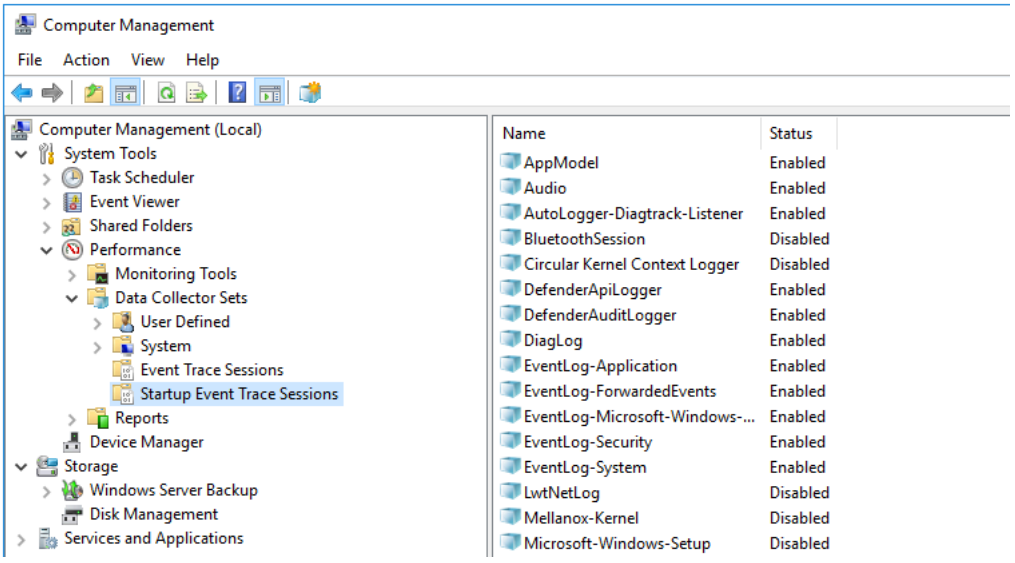
При включенной ротации аналитического журнала события не отображаются. Для просмотра событий в панели **Действия** нажмите на кнопку **Остановить журнал**.



Остановка журнала

5. Запустите Управление компьютером (англ. Computer management) от имени администратора.

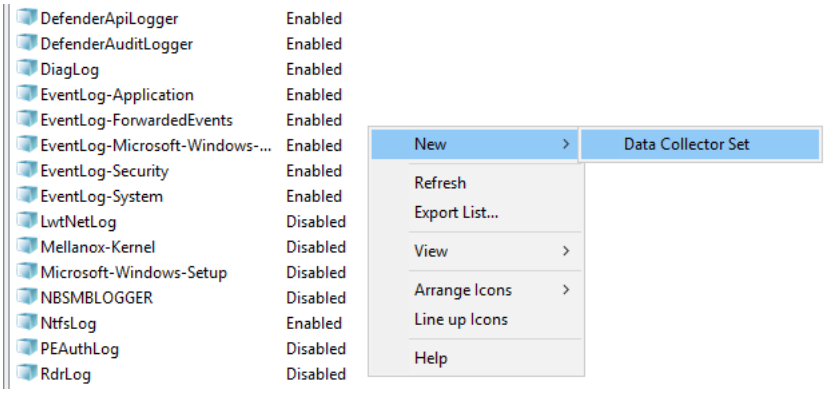
6. В открывшемся окне перейдите в директорию **Служебные программы** → **Производительность** → **Сеансы отслеживания событий запуска**.



Управление компьютером

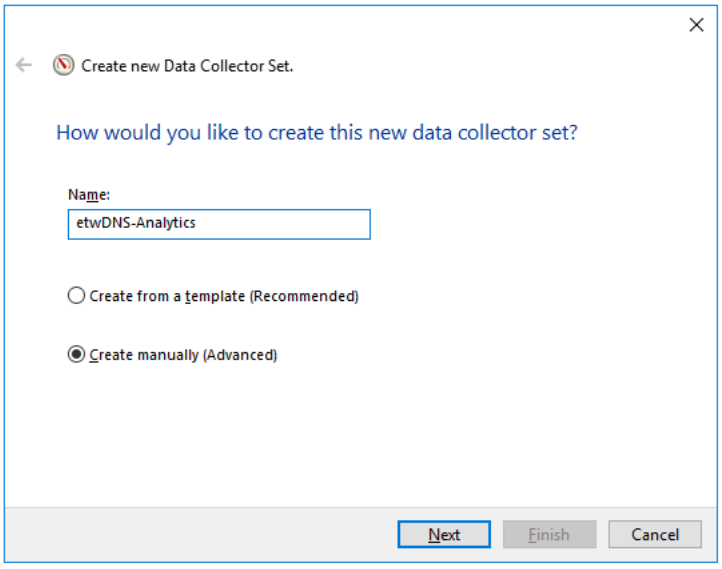
7. Создайте поставщика:

a. Откройте контекстное меню директории **Сеансы отслеживания событий запуска** и выберите пункт **Создать** → **Группа сборщиков данных**.



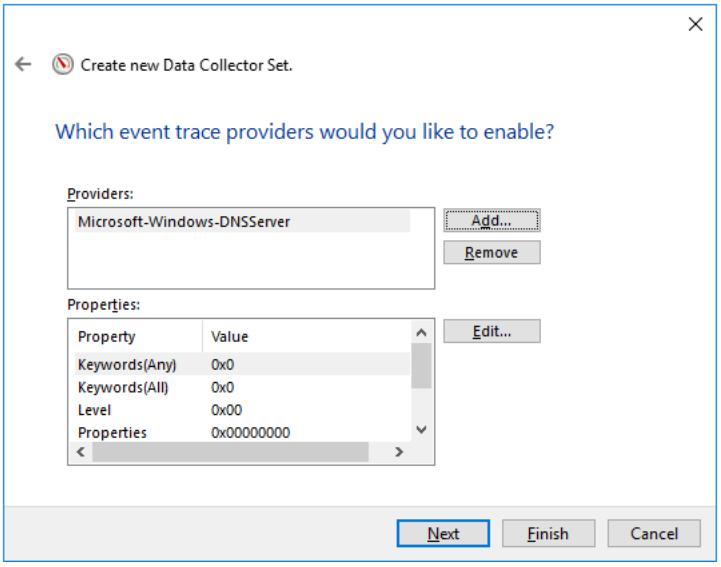
Создание группы сборщиков данных

a. В открывшемся окне введите имя поставщика и нажмите на кнопку **Далее**.



Ввод имени поставщика

a. Нажмите на кнопку **Добавить...** и в открывшемся окне выберите поставщика **Microsoft-Windows-DNSServer**.

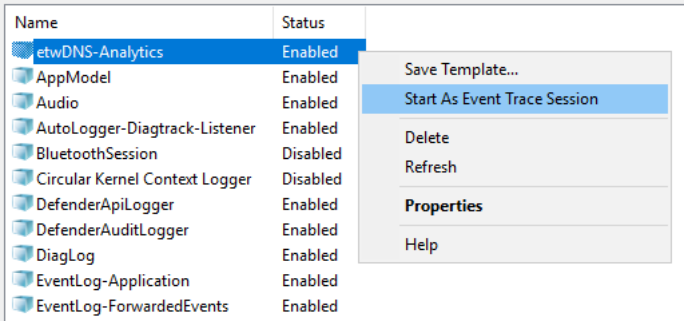


Выбор поставщика

> Агент KUMA с коннектором ETW работает только с System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer.

a. Дважды нажмите на кнопку **Далее**, после чего нажмите на кнопку **Готово**.

8. Откройте контекстное меню созданного поставщика и выберите пункт **Запустить как сеанс отслеживания событий**.



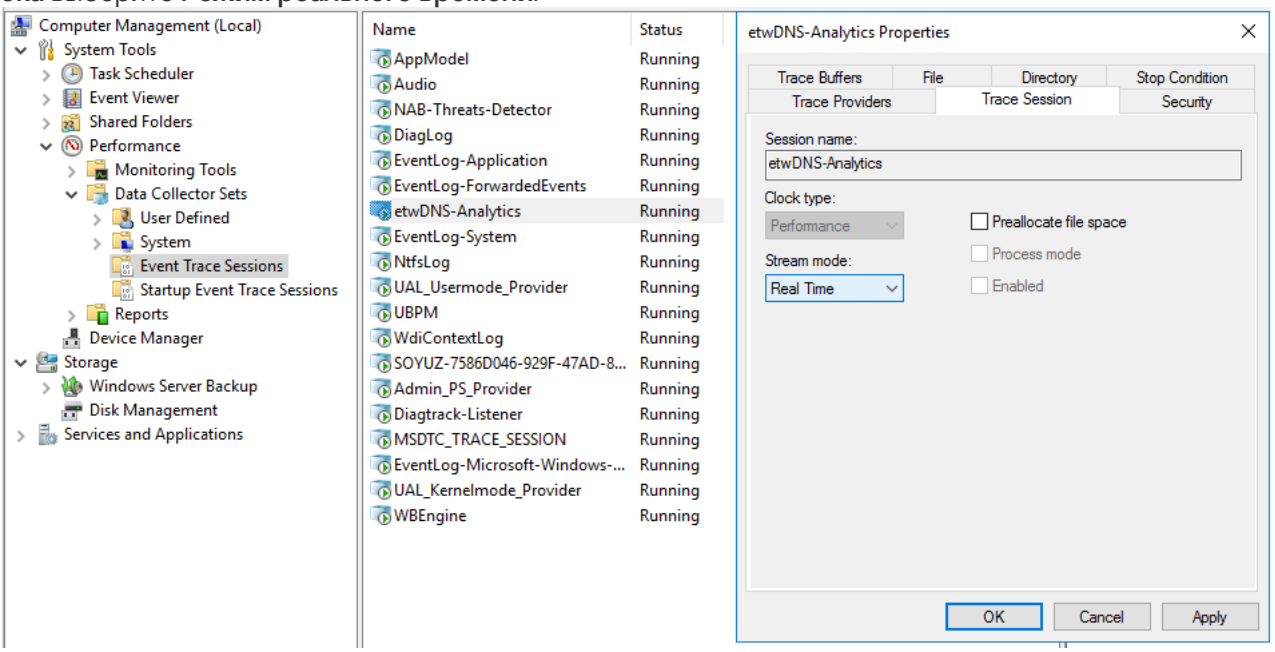
Запуск поставщика

9. Перейдите в директорию **Сеансы отслеживания событий**.

   Отобразятся сеансы отслеживания событий.

10. Откройте контекстное меню созданного сеанса отслеживания событий и выберите пункт **Свойства**.

11. В открывшемся окне выберите вкладку **Сеансы отслеживания** и в раскрывающемся списке **Режим потока** выберите **Режим реального времени**.



Настройка режима потока

12. Нажмите на кнопку **Применить**, после чего нажмите на кнопку **OK**.

    Настройка получения событий DNS-сервера с помощью коннектора ETW будет завершена.

Настройка получения событий PostgreSQL

KUMA позволяет осуществлять мониторинг и проводить аудит событий PostgreSQL на устройствах Linux с помощью rsyslog.

Аудит событий проводится с помощью плагина pgAudit. Плагин поддерживает работу с PostgreSQL версии 9.5 и выше. Подробную информацию о плагине pgAudit см. по ссылке: https://github.com/pgaudit/pgaudit.

Настройка получения событий состоит из следующих этапов:

1. Установка плагина pdAudit.

2. Создание коллектора KUMA для событий PostgreSQL.

   Для получения событий PostgreSQL с помощью rsyslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] PostgreSQL pgAudit syslog**.

3. Установка коллектора в сетевой инфраструктуре KUMA.

4. Настройка сервера источника событий.

5. Проверка поступления событий PostgreSQL в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий PostgreSQL выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Установка плагина pgAudit

Чтобы установить плагин pgAudit:

1. В командном интерпретаторе выполните команды под учетной записью с правами администратора:

   ```
   sudo apt update
   sudo apt -y install postgresql-<версия базы данных PostgreSQL>-pgaudit
   ```

   Версию плагина необходимо выбрать в зависимости от версии PostgresSQL. Информацию о версиях PostgreSQL и необходимых версиях плагина см.по ссылке: https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

   Пример:
   ```
   sudo apt -y install postgresql-12-pgaudit
   ```

2. Найдите конфигурационный файл postgres.conf. Для этого в командной строке PostgresSQL выполните команду:

   ```
   show data_directory;
   ```

   В ответе будет указано расположение конфигурационного файла.

3. Создайте резервную копию конфигурационного файла postgres.conf.

4. Откройте файл postgres.conf и скопируйте или замените имеющиеся значения на указанные ниже.

   ```
   ## pgAudit settings
   shared_preload_libraries = 'pgaudit'
   ## database logging settings
   log_destination = 'syslog'
   ## syslog facility
   syslog_facility = 'LOCAL0'
   ## event ident
   syslog_ident = 'Postgres'
   ## sequence numbers in syslog
   syslog_sequence_numbers = on
   ## split messages in syslog
   syslog_split_messages = off
   ## message encoding
   lc_messages = 'en_US.UTF-8'
   ## min message level for logging
   client_min_messages = log
   ## min error message level for logging
   log_min_error_statement = info
   ## log checkpoints (buffers, restarts)
   log_checkpoints = off
   ## log query duration
   ```

```
log_duration = off
## error description level
log_error_verbosity = default
## user connections logging
log_connections = on
## user disconnections logging
log_disconnections = on
## log prefix format
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status. dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

5. Перезапустите службу PostgreSQL при помощи команды:

   ```
   sudo systemctl restart postgresql
   ```

6. Чтобы загрузить плагин pgAudit в PostgreSQL, в командной строке PostgreSQL выполните команду:

   ```
   CREATE EXTENSION pgaudit;
   ```

Плагин pgAudit установлен.

Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена PostgreSQL, в коллектор:

1. Чтобы проверить, что на сервере источника событий установлен сервис rsyslog, выполните следующую команду под учетной записью с правами администратора:

   ```
   sudo systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. В директории /etc/rsyslog.d/ создайте файл pgsql-to-siem.conf со следующим содержанием:

```
If $programname contains 'Postgres' then @< IP-адрес коллектора >:< порт коллектора >
```

Например:

```
If $programname contains 'Postgres' then @192.168.1.5:1514
```

Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

```
If $programname contains 'Postgres' then @@< IP-адрес коллектора >:< порт коллектора >
```

Сохраните изменения в конфигурационном файле pgsql-to-siem.conf.

3. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

```
$IncludeConfig /etc/pgsql-to-siem.conf
$RepeatedMsgReduction off
```

Сохраните изменения в конфигурационном файле /etc/rsyslog.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Настройка получения событий ИВК Кольчуга-К

Вы можете настроить получение событий системы ИВК Кольчуга-К в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий ИВК Кольчуга-К в KUMA.
2. Создание коллектора KUMA для получения событий ИВК Кольчуга-К.

   Для получения событий ИВК Кольчуга-К с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Kolchuga-K syslog**.

3. Установка коллектора KUMA для получения событий ИВК Кольчуга-К.
4. Проверка поступления событий ИВК Кольчуга-К в KUMA.

   Вы можете проверить, что настройка источника событий ИВК Кольчуга-К выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий ИВК Кольчуга-К в KUMA

Чтобы настроить передачу событий межсетевого экрана ИВК КОЛЬЧУГА-К по syslog в коллектор KUMA:

1. Подключитесь к межсетевому экрану с правами администратора по протоколу SSH.
2. Создайте резервную копию файлов /etc/services и /etc/syslog.conf.
3. В конфигурационном файле /etc/syslog.conf укажите FQDN или IP-адрес коллектора KUMA. Например:

   . @kuma.example.com

   или

   . @192.168.0.100

   Сохраните изменения в конфигурационном файле /etc/syslog.conf.

4. В конфигурационном файле /etc/services укажите порт и протокол, который используется коллектором KUMA. Например:

   syslog 10514/udp

   Сохраните изменения в конфигурационном файле /etc/services.

5. Перезапустите syslog-сервер межсетевого экрана с помощью команды:

   ```
   service syslogd restart
   ```

Настройка получения событий КриптоПро NGate

Вы можете настроить получение событий программы КриптоПро NGate в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий КриптоПро NGate в KUMA.

2. Создание коллектора KUMA для получения событий КриптоПро NGate.

   Для получения событий КриптоПро NGate в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] NGate syslog**.

3. Установка коллектора KUMA для получения событий КриптоПро NGate.

4. Проверка поступления событий КриптоПро NGate в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий КриптоПро NGate выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий КриптоПро NGate в KUMA

Чтобы настроить передачу событий из программы КриптоПро NGate в KUMA:

1. Подключитесь к веб-интерфейсу системы управления NGate.

2. Подключите удаленные syslog-серверы к системе управления. Для этого выполните следующие действия:

   a. Откройте страницу списка syslog-серверов **External Services** → **Syslog Server** → **Add Syslog Server**.

   b. Введите параметры syslog-сервера и нажмите на значок ✔.

3. Выполните привязку syslog-серверов к конфигурации для записи журналов работы кластера. Для этого выполните следующие действия:

   a. В разделе **Clusters** → **Summary** выберите настраиваемый кластер.

   b. На вкладке **Configurations** нажмите на элемент **Configuration** нужного кластера для входа на страницу настроек конфигурации.

c. В поле

Syslog Servers
настраиваемой конфигурации нажмите на кнопку

Assign
.

d. Установите флажки для syslog-серверов, которые вы хотите привязать, и нажмите

на значок ✔.

Вы можете привязать неограниченное число серверов.

Чтобы добавить новые syslog-серверы, нажмите на значок +.

e. Опубликуйте конфигурацию для активации новых настроек.

4. Выполните привязку syslog-серверов к системе управления для записи журналов работы Администратора. Для этого выполните следующие действия:

   a. Выберите пункт меню **Management Center Settings** и на открывшейся странице в блоке **Syslog servers** нажмите на кнопку **Assign**.

   b. В окне **Assign Syslog Servers to Management Center** установите флажок для тех syslog-серверов, которые вы хотите привязать, затем нажмите на значок ✔.

   Вы можете привязать неограниченное количество серверов.

В результате события программы КриптоПро NGate передаются в KUMA.

Настройка получения событий Ideco UTM

Вы можете настроить получение событий программы Ideco UTM в KUMA по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Ideco UTM в KUMA.

2. Создание коллектора KUMA для получения событий Ideco UTM.

   Для получения событий Ideco UTM в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Ideco UTM syslog**.

3. Установка коллектора KUMA для получения событий Ideco UTM.

4. Проверка поступления событий Ideco UTM в KUMA.

   Вы можете проверить, что настройка сервера источника событий Ideco UTM выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий Ideco UTM в KUMA

Чтобы настроить передачу событий из программы Ideco UTM в KUMA:

1. Подключитесь к веб-интерфейсу Ideco UTM под учетной записью с правами администратора.
2. В меню **Пересылка системных сообщений** переведите переключатель **Syslog** в положение **включено**.
3. В параметре **IP-адрес** укажите IP-адрес коллектора KUMA.
4. В параметре Порт введите порт, который прослушивает коллектор KUMA.
5. Нажмите **Сохранить** для применения внесенных изменений.

Передача событий в Ideco UTM в KUMA будет настроена.

Настройка получения событий KWTS

Вы можете настроить получение событий из системы анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (KWTS) в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KWTS в KUMA.

   В зависимости от используемой версии KWTS вы можете использовать одну из следующих инструкций:

   Для KWTS 6.2

   Для KWTS 6.1

   Чтобы настроить передачу событий KWTS в KUMA:

   1. Подключитесь к серверу KWTS по протоколу SSH под учетной записью root.
   2. Перед внесением изменений создайте резервные копии следующих файлов:
      - `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template`
      - `/etc/rsyslog.conf`
   3. Убедитесь, что параметры конфигурационного файла `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template` имеют следующие значения, при необходимости внесите изменения:

      ```
      "siemSettings":
      {
      "enabled": true,
      "facility": "Local5",
      "logLevel": "Info",
      "formatting":
      {
      ```

   4. Сохраните внесенные изменения.

5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл `/etc/rsyslog.conf`:

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local5.* @<<IP-адрес коллектора KUMA>:<Порт коллектора>>
```

Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local5.* @@<<IP-адрес коллектора KUMA>:<Порт коллектора>>
```

6. Сохраните внесенные изменения

7. Перезапустите сервис rsyslog с помощью следующей команды:

```
sudo systemctl restart rsyslog.service
```

8. Перейдите в веб-интерфейс KWTS на вкладку **Параметры** – **Syslog** и включите опцию **Записывать информацию о профиле трафика**.

9. Нажмите **Сохранить**.

2. Настройка экспорта событий в формате CEF.

   Если вы настраиваете получение событий из KWTS 6.2, следуйте инструкции в документации KWTS 6.2, чтобы включить экспорт событий.

3. Создание коллектора KUMA для получения событий KWTS.

   Для получения событий KWTS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KWTS**.

4. Установка коллектора KUMA для получения событий KWTS.

5. Проверка поступления событий KWTS в коллектор KUMA.

   Вы можете проверить, что настройка передачи событий KWTS выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка получения событий KLMS

Вы можете настроить получение событий из системы анализа и фильтрации почтового трафика Kaspersky Linux Mail Server (KLMS) в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. В зависимости от используемой версии KLMS, выберите один из вариантов:
   - Настройка передачи событий KLMS 8 в KUMA.
   - Настройка передачи событий KLMS 10 в KUMA (документация для KLMS 10 доступна только на русском языке).
2. Создание коллектора KUMA для получения событий KLMS.

   Для получения событий KLMS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KLMS syslog CEF**.
3. Установка коллектора KUMA для получения событий KLMS.
4. Проверка поступления событий KLMS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KLMS выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий KLMS в KUMA

Чтобы настроить передачу событий KLMS в KUMA:

1. Подключитесь к серверу KLMS по протоколу SSH и перейдите в меню **Technical Support Mode**.
2. С помощью утилиты klms-control выгрузите настройки в файл settings.xml:

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```
3. Убедитесь, что параметры файла /tmp/settings.xml имеют следующие значения, при необходимости внесите изменения:

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ...
   </siemSettings>
   ```
4. Примените настройки с помощью следующей команды:

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```
5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл /etc/rsyslog.conf.

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   ```

```
$ActionResumeRetryCount -1
local1.* @<< IP-адрес коллектора KUMA >:< порт коллектора >>
```

Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local1.* @@<< IP-адрес коллектора KUMA >:< порт коллектора >>
```

6. Сохраните внесенные изменения.

7. Перезапустите сервис rsyslog с помощью следующей команды:

```
sudo systemctl restart rsyslog.service
```

Настройка получения событий KSMG

Вы можете настроить получение событий из систем анализа и фильтрации почтового трафика Kaspersky Secure Mail Gateway (KSMG) в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KSMG в KUMA.

2. Создание коллектора KUMA для получения событий KSMG.

   Для получения событий KSMG в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSMG**.

3. Установка коллектора KUMA для получения событий KSMG.

4. Проверка поступления событий KSMG в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KSMG выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка получения событий KICS for Networks

Вы можете настроить получение событий из программы Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) версии 4.2 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Создание коннектора KICS for Networks для передачи событий в KUMA.

2. Настройка передачи событий KICS for Networks в KUMA.

3. Создание и установка коллектора KUMA для получения событий KICS for Networks.

4. Проверка поступления событий KICS for Networks в коллектор KUMA.

   Вы можете проверить, что настройка передачи событий KICS for Networks выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Создание коннектора KICS for Networks для передачи событий в KUMA

Чтобы создать коннектор для передачи событий в веб-интерфейсе KICS for Networks:

1. Войдите в веб-интерфейс KICS for Networks под учетной записью администратора.
2. Перейдите в раздел **Параметры** → **Коннекторы**.
3. Нажмите на кнопку **Добавить коннектор**.
4. Укажите следующие параметры:
   a. В раскрывающемся списке **Тип коннектора** выберите значение **SIEM**.
   b. В поле **Имя коннектора** укажите имя для коннектора.
   c. В поле **Адрес Сервера** введите IP-адрес Сервера KICS for Networks.
   d. В раскрывающемся списке **Узел размещения коннектора** выберите узел, на котором вы устанавливаете коннектор.

      Вы можете указать любое имя.
   e. В поле **Имя пользователя** укажите имя пользователя, под которым KUMA будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей KICS for Networks.
   f. В поле **Адрес-SIEM сервера** введите IP-адрес сервера коллектора KUMA.
   g. В поле **Номер порта** введите номер порта коллектора KUMA.
   h. В раскрывающемся списке **Транспортный протокол** выберите одно из следующих значений: **TCP** или **UDP**.
   i. Установите флажок **Разрешить отправку записей аудита**.
   j. Установите флажок **Разрешить отправку записей программы**.
5. Нажмите на кнопку **Сохранить**.

   Коннектор будет создан. Он отобразится в таблице коннекторов KICS for Networks со статусом **Работает**.

Коннектор KICS for Networks для передачи событий в KUMA будет готов к работе.

Настройка передачи событий KICS for Networks в KUMA

Чтобы события безопасности KICS for Networks передавались в KUMA:

1. Войдите в веб-интерфейс KICS for Networks под учетной записью администратора.
2. Перейдите в раздел **Параметры** → **Типы событий**.
3. Установите флажки для типов событий, которые вы хотите передавать в KUMA.

4. Нажмите на кнопку **Выбрать коннекторы**.

5. В открывшемся окне выберите коннектор, созданный для передачи событий в KUMA.

6. Нажмите на кнопку **Ok**.

   Выбранные типы событий будут передаваться в KUMA. В таблице **Типы событий** эти типы событий отмечаются флажком в столбце с названием коннектора.

Создание коллектора KUMA для получения событий KICS for Networks

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий KICS for Networks.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе KUMA вам нужно выполнить следующие требования:

1. На шаге **Транспорт** требуется выбрать тип транспортного протокола, соответствующий типу, выбранному при создании коннектора в KICS for Networks на шаге 4i (TCP или UDP), и номер порта, соответствующий номеру порта, указанному на шаге 4h.

2. На шаге **Парсинг событий** требуется выбрать нормализатор **[OOTB] KICS4Net v3.x**.

3. На шаге **Маршрутизация** нужно убедиться, что в набор ресурсов коллектора добавлены следующие точки назначения:

   - **storage** – используется для передачи данных в хранилище.

   - **correlator** – используется для передачи данных в коррелятор.

   Если точки назначения не добавлены в коллектор, вам нужно создать их.

4. На последнем шаге мастера в нижней части окна отобразится команда, с помощью которой вы можете установить сервис на сервер, предназначенный для получения событий. Вам нужно скопировать эту команду и использовать при установке второй части коллектора.

Настройка получения событий PT NAD

Вы можете настроить получение событий из PT NAD в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий PT NAD в KUMA.

2. Создание коллектора KUMA для получения событий PT NAD.

   Для получения событий PT NAD с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] PT NAD json**.

3. Установка коллектора KUMA для получения событий PT NAD.

4. Проверка поступления событий PT NAD в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий PT NAD выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий PT NAD в KUMA

Настройка передачи событий из PT NAD 11 в KUMA по Syslog включает следующие этапы:

1. Настройка модуля ptdpi-worker@notifier.

2. Настройка отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации.

Настройка модуля ptdpi-worker@notifier

Для включения отправки информации об обнаруженных угрозах информационной безопасности необходимо настроить модуль ptdpi-worker@notifier.

В многосерверной конфигурации инструкцию нужно выполнять на основном сервере.

Чтобы настроить модуль ptdpi-worker@notifier:

1. Откройте файл /opt/ptsecurity/etc/ptdpi.settings.yaml:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. В группе параметров **General settings** раскомментируйте параметр workers и добавьте notifier в список его значений.

   Например:

   ```
   workers: ad alert dns es hosts notifier
   ```

3. Добавьте в конец файла строку вида notifier.yaml.nad_web_url: <URL веб-интерфейса PT NAD>

   Например:

   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```

   Модуль ptdpi-worker@notifier будет использовать указанный URL для формирования ссылок на карточки сессий и активностей при отправке сообщений.

4. Перезапустите сенсор:

   ```
   sudo ptdpictl restart-all
   ```

Модуль ptdpi-worker@notifier настроен.

Настройка syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации

Параметры, перечисленные в следующей инструкции могут отсутствовать в конфигурационном файле. Если параметр отсутствует, вам нужно добавить его в файл самостоятельно.

В многосерверной конфигурации PT NAD настройка выполняется на основном сервере.

Чтобы настроить отправку syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации:

1. Откройте файл /opt/ptsecurity/etc/ptdpi.settings.yaml:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. По умолчанию PT NAD отправляет данные об активностях на русском языке. Чтобы получать данные на английском языке, измените значение параметра notifier.yaml.syslog_notifier.locale на `en`.

   Например:

   ```
   notifier.yaml.syslog_notifier.locale: en
   ```

3. В параметре notifier.yaml.syslog_notifier.addresses добавьте секцию с параметрами отправки событий в KUMA.

   Параметр <Название подключения> может состоять только из букв латинского алфавита, цифр и символа подчеркивания.

   В параметре address необходимо указать IP-адрес коллектора KUMA.

   Остальные параметры можно не указывать, в таком случае будут использоваться значения по умолчанию.

   ```
   notifier.yaml.syslog_notifier.addresses:
   <Название подключения>:
   address: <Для отправки на удаленный сервер – протокол UDP (по умолчанию) или TCP,
   адрес и порт; для локального подключения – сокет домена Unix>
   doc_types: [<Перечисленные через запятую типы сообщений (alert для информации об
   атаках, detection для активностей и reputation для информации об индикаторах
   компрометации). По умолчанию отправляются все типы сообщений>]
   facility: <Числовое значение категории субъекта>
   ident: <Метка ПО>
   <Название подключения>:
   ...
   ```

   Далее представлен пример настройки отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации, отправляемых на два удаленных сервера по протоколам TCP и UDP без записи в локальный журнал:

   ```
   notifier.yaml.syslog_notifier.addresses:
   remote1:
   address: tcp://198.51.100.1:1514
   remote2:
   address: udp://198.51.100.2:2514
   ```

4. Сохраните изменения в файле /opt/ptsecurity/etc/ptdpi.settings.yaml.

5. Перезапустите модуль ptdpi-worker@notifier:

   ```
   sudo ptdpictl restart-worker notifier
   ```

Настройка отправки событий в KUMA по Syslog выполнена.

Настройка получения событий с помощью плагина MariaDB Audit Plugin

KUMA позволяет проводить аудит событий с помощью плагина MariaDB Audit Plugin. Плагин поддерживает работу с MySQL 5.7 и MariaDB. Работа плагина аудита с MySQL 8 не поддерживается. Подробная информация о плагине доступна на официальном веб-сайте MariaDB.

Мы рекомендуем использовать плагин MariaDB Audit Plugin версии 1.2 и выше.

Настройка получения событий состоит из следующих этапов:

1. Настройка плагина MariaDB Audit Plugin для передачи событий MySQL и настройка Syslog-сервера для отправки событий.

2. Настройка плагина MariaDB Audit Plugin для передачи событий MariaDB и настройка Syslog-сервера для отправки событий.

3. Создание коллектора KUMA для событий MySQL 5.7 и MariaDB.

   Для получения событий MySQL 5.7 и MariaDB с помощью плагина MariaDB Audit Plugin в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] MariaDB Audit Plugin syslog**.

4. Установка коллектора в сетевой инфраструктуре KUMA.

5. Проверка поступления событий MySQL и MariaDB в коллектор KUMA.

   Чтобы проверить, что настройка сервера источника событий MySQL и MariaDB выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка плагина MariaDB Audit Plugin для передачи событий MySQL

Плагин MariaDB Audit Plugin поддерживается для MySQL 5.7 версии до 5.7.30 и поставляется в комплекте с MariaDB.

Чтобы настроить передачу событий MySQL 5.7 с помощью плагина MariaDB Audit Plugin:

1. Скачайте дистрибутив MariaDB и распакуйте его.

   Дистрибутив MariaDB доступен на официальном веб-сайте MariaDB. Операционная система дистрибутива MariaDB должна совпадать с операционной системой, на которой функционирует MySQL 5.7.

2. Подключитесь к MySQL 5.7 под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

3. Чтобы получить директорию, в которой расположены плагины MySQL 5.7, в командной строке MySQL 5.7 выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

4. В директории, полученной на шаге 3, скопируйте плагин MariaDB Audit Plugin из директории `<директория, куда был разархивирован дистрибутив>/mariadb-server-<версия>/lib/plugins/server_audit.so`.

5. В командном интерпретаторе операционной системы выполните команду:

   ```
   chmod 755 <директория, куда был разархивирован дистрибутив>server_audit.so
   ```

   Например:

   ```
   chmod 755 /usr/lib64/mysql/plugin/server_audit.so
   ```

6. В командном интерпретаторе MySQL 5.7 выполните команду:

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

7. Создайте резервную копию конфигурационного файла /etc/mysql/mysql.conf.d/mysqld.cnf.

8. В конфигурационном файле /etc/mysql/mysql.conf.d/mysqld.cnf в разделе `[mysqld]` добавьте следующие строки:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

9. Сохраните изменения в конфигурационном файле.

10. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

    - `systemctl restart mysqld` – для системы инициализации systemd.
    - `service mysqld restart` – для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MySQL 5.7 завершена. При необходимости вы можете выполнить следующие команды в командной строке MySQL 5.7:

- `show plugins` – для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` – для проверки текущих настроек аудита.

Настройка плагина MariaDB Audit Plugin для передачи событий MariaDB

Плагин MariaDB Audit Plugin входит в состав дистрибутива MariaDB, начиная с версий 5.5.37 и 10.0.10.

Чтобы настроить передачу событий MariaDB с помощью плагина MariaDB Audit Plugin:

1. Подключитесь к MariaDB под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

2. Чтобы проверить, что плагин есть в директории, где размещены плагины операционной системы, в командной строке MariaDB выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

3. В командном интерпретаторе операционной системы выполните команду:

   ```
   ll <директория, полученная в результате выполнения предыдущей команды> | grep server_audit.so
   ```

   Если вывод команды пуст и плагина нет в директории, вы можете скопировать плагин MariaDB Audit Plugin в эту директорию или использовать более новую версию MariaDB.

4. В командном интерпретаторе MariaDB выполните команду:

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

5. Создайте резервную копию конфигурационного файла /etc/mysql/my.cnf.

6. В конфигурационном файле /etc/mysql/my.cnf в разделе `[mysqld]` добавьте следующие строки:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

7. Сохраните изменения в конфигурационном файле.

8. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

   - `systemctl restart mariadb` – для системы инициализации systemd.
   - `service mariadb restart` – для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MariaDB завершена. При необходимости вы можете выполнить следующие команды в командной строке MariaDB:

- `show plugins` – для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` – для проверки текущих настроек аудита.

Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена MySQL или MariaDB, в коллектор:

1. Перед внесением изменений создайте резервную копию конфигурационного файла /etc/rsyslog.conf.

2. Для отправки событий по протоколу UDP добавьте в конфигурационный файл /etc/rsyslog.conf строку:

   ```
   *.* @<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
   ```

   Например:

```
*.* @192.168.1.5:1514
```

Если вы хотите отправлять события по протоколу TCP, строка должна выглядеть следующим образом:

```
*.* @@192.168.1.5:2514
```

Сохраните изменения в конфигурационном файле /etc/rsyslog.conf.

3. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Настройка получения событий СУБД Apache Cassandra

KUMA позволяет получать информацию о событиях Apache Cassandra.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Apache Cassandra в KUMA.

2. Создание коллектора KUMA для событий Apache Cassandra.

   Для получения событий Apache Cassandra в мастере установки коллектора KUMA необходимо выполнить следующие действия: на шаге **Транспорт** выберите коннектор типа **file**, на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Apache Cassandra file**.

3. Установка коллектора в сетевой инфраструктуре KUMA.

4. Проверка поступления событий Apache Cassandra в коллектор KUMA.

   Чтобы проверить, что настройка сервера источника событий Apache Cassandra выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка журналирования событий Apache Cassandra в KUMA

Чтобы настроить журналирование событий Apache Cassandra в KUMA:

1. Убедитесь, что на сервере, где установлена Apache Cassandra, есть 5 ГБ свободного дискового пространства.

2. Подключитесь к серверу Apache Cassandra под учетной записью с правами администратора.

3. Перед внесением изменений создайте резервные копии следующих конфигурационных файлов:

   - /etc/cassandra/cassandra.yaml

   - /etc/cassandra/logback.xml

4. Убедитесь, что параметры конфигурационного файла /etc/cassandra/cassandra.yaml имеют следующие значения, при необходимости внесите изменения:

   a. в секции `audit_logging_options` присвойте параметру `enabled` значение `true.`

   b. в секции `logger` присвойте параметру `class_name` значение `FileAuditLogger.`

5. В конфигурационный файл /etc/cassandra/logback.xml добавьте следующие строки:

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
<file>${cassandra.logdir}/audit/audit.log</file>
<rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
<!-- rollover daily -->
<fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-dd}.%i.zip</fileNamePattern>
<!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB -->
<maxFileSize>50MB</maxFileSize>
<maxHistory>30</maxHistory>
<totalSizeCap>5GB</totalSizeCap>
</rollingPolicy>
<encoder>
<pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', ' '}%n</pattern>
</encoder>
</appender>
<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
<appender-ref ref="AUDIT"/>
</logger>
```

6. Сохраните изменения в конфигурационном файле.

7. Перезапустите службу Apache Cassandra с помощью следующих команд:

   a. `sudo systemctl stop cassandra.service`

   b. `sudo systemctl start cassandra.service`

8. После перезапуска проверьте статус Apache Cassandra с помощью следующей команды:

   ```
   sudo systemctl status cassandra.service
   ```

   Убедитесь, что в выводе команды есть последовательность символов:

   ```
   Active: active (running)
   ```

Настройка передачи событий Apache Cassandra завершена. События будут располагаться в директории /var/log/cassandra/audit/, в файле audit.log (${cassandra.logdir}/audit/audit.log).

Настройка получения событий FreeIPA

Вы можете настроить получение событий FreeIPA в KUMA по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий FreeIPA в KUMA.

2. Создание коллектора KUMA для получения событий FreeIPA.

   Для получения событий FreeIPA в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] FreeIPA**.

3. Установка коллектора KUMA в сетевой инфраструктуре.

4. Проверка поступления событий FreeIPA в KUMA.

   Чтобы проверить, что настройка сервера источника событий FreeIPA выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка передачи событий FreeIPA в KUMA

Чтобы настроить передачу событий FreeIPA в KUMA по протоколу Syslog в формате JSON:

1. Подключитесь к серверу FreeIPA по протоколу SSH под учетной записью с правами администратора.

2. В директории /etc/rsyslog.d/ создайте файл freeipa-to-siem.conf.

3. В конфигурационный файл /etc/rsyslog.d/freeipa-to-siem.conf добавьте следующие строки:

```
$ModLoad imfile
input(type="imfile"
File="/var/log/httpd/error_log"
Tag="tag_FreeIPA_log_httpd"
facility="local3")
input(type="imfile"
File="/var/log/dirsrv/slapd-*/audit"
Tag="tag_FreeIPA_log_audit"
StartMsg.regex="^time:"
facility="local3")
input(type="imfile"
File="/var/log/dirsrv/slapd-*/errors"
Tag="tag_FreeIPA_log_errors"
facility="local3")
input(type="imfile"
File="/var/log/dirsrv/slapd-*/access"
Tag="tag_FreeIPA_log_access"
facility="local3")
input(type="imfile"
File="/var/log/krb5kdc.log"
Tag="tag_FreeIPA_log_krb5kdc"
facility="local3")
```

```
template(name="ls_json" type="list" option.json="on") {
constant(value="{")
constant(value="\"@timestamp\":\"") property(name="timegenerated"
dateFormat="rfc3339")
constant(value="\",\"@version\":\"1")
constant(value="\",\"message\":\"") property(name="msg")
constant(value="\",\"host\":\"") property(name="fromhost")
constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
constant(value="\",\"logsource\":\"") property(name="fromhost")
constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
constant(value="\",\"severity\":\"") property(name="syslogseverity")
constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
constant(value="\",\"facility\":\"") property(name="syslogfacility")
constant(value="\",\"program\":\"") property(name="programname")
constant(value="\",\"pid\":\"") property(name="procid")
constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
constant(value="\"}\n")
}
if $syslogtag contains 'tag_FreeIPA_log' then {
action(type="omfwd"
target="< IP-адрес коллектора KUMA >"
port="< порт коллектора KUMA >"
protocol="< udp или tcp >"
template="ls_json")
stop
}
```

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

```
$IncludeConfig /etc/rsyslog.d/freeipa-to-siem.conf
$RepeatedMsgReduction off
```

5. При необходимости выключите локальную запись событий FreeIPA, выполнив следующие действия:

   a. Откройте на редактирование конфигурационный файл rsyslog /etc/rsyslog.conf или файл правил по умолчанию /etc/rsyslog.d/50-default.conf.

   b. Найдите в файле строку, отвечающую за запись системных событий, и добавьте в нее параметр `local3.none`, так как в конфигурационном файле /etc/rsyslog.d/freeipa-to-siem.conf параметру `facility` присвоено значение `local3`. Измененная строка должна выглядеть следующим образом:

      ```
      *.info;mail.none;authpriv.none;cron.none;local3.none /var/log/messages
      ```

      Если значение параметра `facility local3` уже используется другой программой на сервере, измените значение параметра `facility` для FreeIPA в файле /etc/rsyslog.d/freeipa-to-siem.conf на другое значение и внесите соответствующие правки в выбранном конфигурационном файле rsyslog.

   c. Сохраните изменения.

6. Сохраните изменения в конфигурационном файле /etc/rsyslog.d/freeipa-to-siem.conf.

7. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Настройка получения событий VipNet TIAS

Вы можете настроить получение событий VipNet TIAS в KUMA по протоколу syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий VipNet TIAS в KUMA.

2. Создание коллектора KUMA для получения событий VipNet TIAS.

   Для получения событий VipNet TIAS с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Syslog-CEF**.

3. Установка коллектора KUMA для получения событий VipNet TIAS.

4. Проверка поступления событий VipNet TIAS в KUMA.

   Вы можете проверить, что настройка сервера источника событий VipNet TIAS выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий VipNet TIAS в KUMA

Чтобы настроить передачу событий VipNet TIAS в KUMA по протоколу syslog:

1. Подключитесь к веб-интерфейсу VipNet TIAS под учетной записью с правами администратора.

2. Перейдите в раздел **Управление** – **Интеграции**.

3. На странице **Интеграция** перейдите на вкладку Syslog.

4. На панели инструментов списка принимающих серверов нажмите **Новый сервер**.

5. В открывшейся карточке нового сервера выполните следующие действия:

   1. В поле **Адрес сервера** укажите IP-адрес или доменное имя коллектора KUMA.

      Например, 10.1.2.3 или syslog.siem.ru

   2. В поле **Порт** укажите входящий порт коллектора KUMA. По умолчанию указан порт 514.

   3. В списке **Протокол** выберите протокол транспортного уровня, который прослушивает коллектор KUMA. По умолчанию выбран протокол UDP.

   4. В списке **Организация** с помощью флажков выберите организации инфраструктуры ViPNet TIAS.

      Сообщения будут отправляться только по инцидентам, обнаруженным на основании событий, полученных от сенсоров выбранных организаций инфраструктуры.

5. В списке **Статус** с помощью флажков выберите статусы инцидентов.

   Сообщения будут отправляться только при назначении инцидентам выбранных статусов.

6. В списке **Уровень важности** с помощью флажков выберите уровни важности инцидентов.

   Сообщения будут отправляться только об инцидентах выбранных уровней важности. По умолчанию в списке выбран только высокий уровень важности.

7. В списке **Язык интерфейса** выберите язык, на котором вы хотите получать информацию об инцидентах в сообщениях. По умолчанию выбран русский язык.

6. Нажмите кнопку **Добавить**.

7. На панели инструментов списка включите переключатель **Не передавать информацию об инцидентах в формате CEF**.

   В результате при обнаружении новых и изменении статусов ранее выявленных инцидентов, в зависимости от выбранных при настройке статусов, будет выполняться передача соответствующей информации на указанные адреса принимающих серверов по протоколу syslog в формате CEF.

8. Нажмите **Сохранить изменения**.

Настройка отправки событий в коллектор KUMA выполнена.

Настройка получения событий Nextcloud

Вы можете настроить получение событий программы Nextcloud 26.0.4 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий Nextcloud.

2. Настройка Syslog-сервера для отправки событий.

   Для передачи событий от сервера в коллектор используется сервис rsyslog.

3. Создание коллектора KUMA для получения событий Nextcloud.

   Для получения событий Nextcloud в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Nextcloud syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

4. Установка коллектора KUMA для получения событий Nextcloud.

5. Проверка поступления событий Nextcloud в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Nextcloud выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка аудита событий Nextcloud

Чтобы настроить передачу событий Nextcloud в KUMA:

1. На сервере, на котором установлена программа Nextcloud, создайте резервную копию конфигурационного файла `/home/localuser/www/nextcloud/config/config.php`.

2. Отредактируйте конфигурационный файл Nextcloud `/home/localuser/www/nextcloud/config/config.php`.

3. Измените значения следующих параметров на приведенные ниже:

```
'log_type' => 'syslog',
'syslog_tag' => 'Nextcloud',
'logfile' => '',
'loglevel' => 0,
'log.condition' => [
'apps' => ['admin_audit'],
],
```

4. Перезагрузите сервис Nextcloud с помощью команды:

```
sudo service restart nextcloud
```

Настройка отправки событий в коллектор KUMA будет выполнена.

Настройка Syslog-сервера для отправки событий Nextcloud

Чтобы настроить передачу событий от сервера, на котором установлена программа Nextcloud, в коллектор:

1. В каталоге /etc/rsyslog.d/ создайте файл Nextcloud-to-siem.conf со следующим содержанием:

```
If $programname contains 'Nextcloud' then @<IP-адрес коллектора>:<порт коллектора>
```

Пример:
```
If $programname contains 'Nextcloud' then @192.168.1.5:1514
```

Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

```
If $programname contains 'Nextcloud' then @@<IP-адрес коллектора>:<порт коллектора>
```

2. Сохраните изменения в конфигурационном файле Nextcloud-to-siem.conf.

3. Создайте резервную копию файла /etc/rsyslog.conf.

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

```
$IncludeConfig /etc/Nextcloud-to-siem.conf
$RepeatedMsgReduction off
```

5. Сохраните внесенные изменения.

6. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Передача событий Nextcloud в коллектор будет настроена.

Настройка получения событий Snort

Вы можете настроить получение событий программы Snort версии 3 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Snort.

2. Создание коллектора KUMA для получения событий Snort.

   Для получения событий Snort в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Snort 3 json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Snort.

4. Проверка поступления событий Snort в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Snort выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка журналирования событий Snort

> Убедитесь, что на сервере, на котором запущен Snort, есть минимум 500 МБ свободного дискового пространства для сохранения одного журнала событий Snort.
> По достижении объема журнала 500 МБ Snort автоматически создаст новый файл, в имени которого будет указано текущее время в формате unixtime.
> Мы рекомендуем отслеживать заполнение дискового пространства.

Чтобы настроить журналирование событий Snort:

1. Подключитесь к серверу, на котором установлен Snort, под учетной записью с правами администратора.

2. Измените конфигурационный файл Snort. Для этого в командном интерпретаторе выполните команду:

   ```
   sudo vi /usr/local/etc/snort/snort.lua
   ```

3. В конфигурационном файле измените содержимое блока alert_json:

   ```
   alert_json =
   {
   file = true,
   limit = 500,
   fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
   eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls
   \
   ```

```
pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
}
```

4. Для завершения настройки выполните следующую команду:

```
sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l
/var/log/snort -i <название интерфейса, который прослушивает Snort> -m 0x1b
```

В результате события Snort будут записываться в файл /var/log/snort/alert_json.txt.

Настройка получения событий Suricata

Вы можете настроить получение событий программы Suricata версии 7.0.1 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Suricata в KUMA.
2. Создание коллектора KUMA для получения событий Suricata.

   Для получения событий Suricata в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Suricata json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Suricata.
4. Проверка поступления событий Suricata в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Suricata выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка аудита событий Suricata

Чтобы настроить журналирование событий Suricata:

1. Подключитесь по протоколу SSH к серверу, обладающему административными учетными записями.
2. Создайте резервную копию файла /etc/suricata/suricata.yaml.
3. Установите в конфигурационном файле /etc/suricata/suricata.yaml в секции eve-log следующие значения:

```
- eve-log:
enabled: yes
filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
filename: eve.json
```

4. Сохраните изменения в файле конфигурации /etc/suricata/suricata.yaml.

В результате события Suricata будут записываться в файл /usr/local/var/log/suricata/eve.json.

Suricata не поддерживает ограничение размера файла с событиями eve.json. При необходимости вы можете контролировать размер журнала с помощью ротации. Например, для настройки ежечасной ротации журнала добавьте в конфигурационный файл следующие строки:

```
outputs:

- eve-log:

filename: eve-%Y-%m-%d-%H:%M.json

rotate-interval: hour
```

Настройка получения событий FreeRADIUS

Вы можете настроить получение событий программы FreeRADIUS версии 3.0.26 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий FreeRADIUS.
2. Настройка Syslog-сервера для отправки событий FreeRADIUS.
3. Создание коллектора KUMA для получения событий FreeRADIUS.

   Для получения событий FreeRADIUS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] FreeRADIUS syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.
4. Установка коллектора KUMA для получения событий FreeRADIUS.
5. Проверка поступления событий FreeRADIUS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий FreeRADIUS выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка аудита событий FreeRADIUS

Чтобы настроить аудит событий в системе FreeRADIUS:

1. Подключитесь к серверу, на котором установлена система FreeRADIUS, под учетной записью с правами администратора.
2. Создайте резервную копию конфигурационного файла FreeRADIUS с помощью команды:

   ```
   sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
   ```
3. Откройте конфигурационный файл FreeRADIUS для редактирования с помощью команды:

   ```
   sudo nano /etc/freeradius/3.0/radiusd.conf
   ```
4. В секции log измените параметры следующим образом:

   ```
   destination = syslog
   syslog_facility = daemon
   ```

```
stripped_names = no
auth = yes
auth_badpass = yes
auth_goodpass = yes
```

5. Сохраните конфигурационный файл.

Аудит событий FreeRADIUS будет настроен.

Настройка Syslog-сервера для отправки событий FreeRADIUS

Для передачи событий от сервера FreeRADIUS в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлен FreeRADIUS, в коллектор:

1. В каталоге /etc/rsyslog.d/ создайте файл FreeRADIUS-to-siem.conf и добавьте в него следующую строку:

   ```
   If $programname contains 'radiusd' then @<IP-адрес коллектора>:<порт коллектора>
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'radiusd' then @@<IP-адрес коллектора>:<порт коллектора>
   ```

2. Создайте резервную копию файла /etc/rsyslog.conf.

3. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/FreeRADIUS-to-siem.conf
   $RepeatedMsgReduction off
   ```

4. Сохраните внесенные изменения.

5. Перезапустите службу rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Передача событий от сервера FreeRADIUS в коллектор KUMA будет настроена.

Настройка получения событий VMware vCenter

Вы можете настроить получение событий VMware vCenter в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка подключения к VMware vCenter.

2. Создание коллектора KUMA для получения событий VMware vCenter.

   Для получения событий VMWare Vcenter в мастере установки коллектора на шаге **Транспорт** выберите тип коннектора vmware. Укажите обязательные параметры:

   - URL, по которому доступен API VMware, например, https://vmware-server.com:6440.

   - Учетные данные VMware – секрет, в котором указаны логин и пароль для подключения к API VMware.

На шаге **Парсинг событий** выберите нормализатор **[OOTB] VMware vCenter API**.

3. Установка коллектора KUMA для получения событий VMWare Vcenter.

4. Проверка поступления событий VMWare Vcenter в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий VMWare Vcenter выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка подключения к VMware vCenter

Чтобы настроить подключение к VMware Vcenter для получения событий:

1. Подключитесь к веб-интерфейсу VMware Vcenter под учетной записью с правами администратора.

2. Перейдите в раздел **Security&Users** и выберите **Users**.

3. Создайте учетную запись пользователя.

4. Перейдите в раздел **Roles** и назначьте созданной учетной записи роль **Read-only: See details of objects, but not make changes**.

   Учетные данные этой записи вы будете использовать в секрете коллектора.

   Более подробная информация о создании учетных записей представлена в документации системы VMware Vcenter.

Настройка подключения к VMware vCenter для получения событий выполнена.

Настройка получения событий zVirt

Вы можете настроить получение событий программы zVirt версии 3.1 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий zVirt в KUMA.

2. Создание коллектора KUMA для получения событий zVirt.

   Для получения событий zVirt в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] OrionSoft zVirt syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

3. Установка коллектора KUMA для получения событий zVirt.

4. Проверка поступления событий zVirt в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий zVirt выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка передачи событий zVirt

Система zVirt может передавать события во внешние системы в режиме установки Hosted Engine.

Чтобы настроить передачу событий из zVirt в KUMA:

1. В веб-интерфейсе zVirt в разделе **Ресурсы** выберите **Виртуальные машины**.
2. Выделите машину, на которой запущена виртуальная машина HostedEngine, и нажмите **Изменить**.
3. В окне **Изменить виртуальную машину** перейдите в раздел **Журналирование**.
4. Установите флажок **Определить адрес Syslog-сервера**.
5. В поле ввода укажите данные коллектора в следующем формате: `<IP-адрес или FQDN коллектора KUMA>: <порт коллектора KUMA>`.
6. Если вы хотите использовать протокол TCP вместо UDP для передачи журналов, установите флажок **Использовать TCP-соединение**.

Передача событий будет настроена.

Настройка получения событий Zeek IDS

Вы можете настроить получение событий программы Zeek IDS версии 1.8 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Преобразование формата журнала событий Zeek IDS.

   Нормализатор KUMA поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор KUMA файлы журналов нужно преобразовать в формат JSON.

2. Создание коллектора KUMA для получения событий Zeek IDS.

   При создании коллектора в веб-интерфейсе KUMA на шаге **Парсинг событий** выберите нормализатор **[OOTB] ZEEK IDS json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Zeek IDS.
4. Проверка поступления событий Zeek IDS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Zeek IDS выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Преобразование формата журнала событий Zeek IDS

По умолчанию события Zeek IDS записываются в файлы в каталог /opt/zeek/logs/current.

Нормализатор [OOTB] ZEEK IDS json file поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор KUMA файлы журналов нужно преобразовать в формат JSON.

> Эту процедуру нужно повторять каждый раз перед получением событий Zeek IDS.

Чтобы преобразовать формат журнала событий Zeek IDS:

1. Подключитесь к серверу, на котором установлена программа Zeek IDS, под учетной записью с правами администратора.

2. Создайте директорию, где будут храниться журналы событий в формате JSON, с помощью команды:

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. Перейдите в эту директорию с помощью команды:

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. Выполните команду, которая с помощью утилиты jq преобразует исходный формат журнала событий к необходимому:

   ```
   jq . -c <путь к файлу журнала, формат которого нужно изменить> >> <название нового файла>.log
   ```

   Пример:
   ```
   jq . -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

В результате выполнения команды в директории /opt/zeek/logs/zeek-json будет создан новый файл, если такого ранее не существовало. Если такой файл уже был в текущей директории, то в конец файла будет добавлена новая информация.

Настройка получения событий Windows с помощью Kaspersky Endpoint Security для Windows

В Kaspersky Endpoint Security for Windows, начиная с версии 12.6, есть возможность отправлять события из журналов Windows в коллектор KUMA. Это позволяет получать в KUMA события из журналов Windows со всех хостов, на которых установлен Kaspersky Endpoint Security for Windows версии 12.6 и выше, без установки агентов KUMA на эти хосты.

Kaspersky Endpoint Security for Windows версии 12.6–12.10 поддерживает ограниченный набор EventID продуктов компании Microsoft.
В версиях Kaspersky Endpoint Security for Windows 12.6-12.12 схожие по параметрам события фильтруются и отправляется первое из них, а последующие аналогичные события не передаются. При массовом возникновении однотипных событий некоторые из них будут отправлены, для этого может потребоваться появление порядка сотен и тысяч схожих событий. При этом отличающееся событие, например, при входе другого пользователя, будет отправлено. Логика фильтрации определена экспертами "Лаборатории Касперского" и позволяет снизить объем передаваемых событий без потери данных, необходимых для обнаружения атак.

Для активации функциональности требуется:

- иметь действующую лицензию KUMA.
- использовать Kaspersky Security Center 14.2 и выше.
- использовать Kaspersky Endpoint Security for Windows 12.6 или выше.

Настройка получения событий состоит из следующих этапов:

1. **Импорт нормализатора в KUMA**

   В KUMA должно быть настроено получение обновлений через серверы обновлений "Лаборатории Касперского".

   В разделе **Ресурсы** нажмите **Импортировать ресурсы** и выберите **[OOTB] Microsoft Products via KES WIN** в списке доступных к установке нормализаторов.

2. **Создание коллектора KUMA для получения событий Windows**

   В зависимости от используемой версии Kaspersky Endpoint Security for Windows выполните следующие действия:

   - Если вы используете Kaspersky Endpoint Security for Windows версии 12.6–12.10, на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите нормализатор **[OOTB] Microsoft Products via KES WIN** и на шаге **Фильтрация событий** выберите фильтр **[OOTB] Microsoft Products via KES WIN - Event filter for collector**.

   - Если вы используете Kaspersky Endpoint Security for Windows версии 12.11 и выше, на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите один из следующих нормализаторов:

     - Для KUMA версии 3.2–4.0 – **[OOTB] Microsoft Products via KES WIN NG for KUMA 3.2**.

     - Для KUMA версии 4.0.1 и выше – **[OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1**.

3. **Запрос ключа в Службе технической поддержки**

   Если в вашей лицензии не было ключа активации функционала отправки журналов Windows в коллектор KUMA, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия KUMA и используется Kaspersky Endpoint Security for Windows версии 12.6. Мы планируем активировать функционал отправки журналов Windows в коллектор KUMA. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям KUMA не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено 2 ключа с лицензиями для KUMA и для активирования функционала Kaspersky Endpoint Security for Windows.

   В ответ на письмо вам будет предоставлен файл ключа.

4. **Настройка на стороне Kaspersky Security Center и Kaspersky Endpoint Security for Windows**

   Файл ключа, активирующий функционал отправки событий Windows в коллекторы KUMA, необходимо импортировать в Kaspersky Security Center и распространить по конечным устройствам Kaspersky Endpoint Security в соответствии с инструкцией. Также необходимо в политике Kaspersky Endpoint Security добавить адреса серверов KUMA и настроить сетевые параметры подключения.

5. **Проверка поступления событий Windows в коллектор KUMA**

   Вы можете проверить, что настройка сервера источника событий Windows выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Перечень событий продуктов Microsoft, которые Kaspersky Endpoint Security for Windows версии 12.6–12.10 передает в KUMA, приведен в таблице ниже.

Журнал событий	Идентификатор события
System	12 13 7040 7045 42 104 107 109 1074 6005 6006 7034 7036 8003

Журнал событий	Идентификатор события
Security	1102 4614 4649 4696 4698 4704 4706 4713 4715 4717 4720 4723 4724 4725 4726 4727 4728 4729 4738 4739 4740 4741 4742 4756 4757 4765 4766 4767 4768 4769 4770 4771 4775 4776 4778 4780 4781 4794 4817 4876 4877 4882 4885 4886 4887 4890 4891 4898 4904 4905 4928 4950 4964 5136 5137 5138 5139 5141 5142 5143 5144 5155 5376 5377 5632 5888 5890 6416 4622 4648 4672 4697 4702 4719 4732 4733

Журнал событий	Идентификатор события
	4798 4946 4947 4948 4949 5145 4616 4625 4663 4624 4799 5140 1008 1105 2722 4615 4618 4626 4627 4634 4647 4653 4654 4656 4657 4658 4659 4660 4661 4664 4666 4667 4670 4673 4674 4688 4689 4690 4691 4692 4693 4694 4695 4699 4700 4701 4703 4705 4707 4714 4716 4718 4730 4731 4734 4737 4743 4744 4745 4746 4747 4748 4749 4750 4751 4752 4753 4754 4755 4758 4759 4760 4761 4762 4763 4764

Журнал событий	Идентификатор события
	4772
	4773
	4774
	4777
	4779
	4782
	4783
	4784
	4785
	4786
	4787
	4788
	4789
	4790
	4791
	4792
	4793
	4797
	4800
	4801
	4802
	4803
	4818
	4819
	4820
	4821
	4822
	4823
	4824
	4825
	4826
	4865
	4866
	4867
	4868
	4869
	4870
	4871
	4872
	4873
	4874
	4875
	4883
	4884
	4888
	4892
	4893
	4896
	4906
	4907
	4908
	4911
	4912
	4913
	4929
	4930
	4931
	4932
	4933
	4935
	4944
	4945
	4951
	4953
	4956
	4957
	4958
	4981
	4982
	4983
	4984
	4985
	5024
	5031
	5033
	5039

Журнал событий	Идентификатор события
	5049 5051 5056 5057 5058 5059 5060 5061 5063 5064 5065 5066 5067 5068 5069 5070 5071 5122 5123 5146 5147 5152 5153 5154 5156 5157 5158 5159 5168 5378 5379 5380 5381 5382 5447 5448 5451 5452 5459 5461 5472 5474 5477 5478 5483 5484 5633 6144 6145 6272 6273 6274 6276 6278 6279 6280 6281 6410 6419 6420 6421 6422 6423 6424 6889

Журнал событий	Идентификатор события
PowerShell	4100 4103 4104 4105 4106 8193 8194 8197 24577 24595 24596 24597 24598 24599 53249 53250 53504
MS SQL Server	615 919 958 1945 2007 2812 3406 3407 3421 3454 5084 5579 5701 5703 6253 8128 9013 9666 15268 15457 17104 17110 17111 17125 17137 17152 17164 17176 17177 17199 17201 17550 17551 17561 17663 18264 18265 18456 18488 18496 19030 19031 19032 26022 26037 26048 26067 33090 49903 49904

Журнал событий	Идентификатор события
Microsoft Defender	1006 1015 1116 1117 1000 1001 2000 5000 5001 5002 5004 5007 5010 5012
Terminal Server	1149 21 22 24 25 39 40
Microsoft Active Directory Federation Service (AD FS)	106 217 251 335 342 349 358 364 381 385 400 401 417 424 435 436
Sysmon	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 255
Microsoft Active Directory Domain Service (AD DS)	1213 1317 1644 2041 2889

Настройка получения событий Linux с помощью Kaspersky Endpoint Security для Linux

В Kaspersky Endpoint Security для Linux, начиная с версии 12.2, есть возможность отправлять события из журналов Linux в коллектор KUMA. Это позволяет получить в KUMA события из журналов Linux со всех хостов, на которых установлен Kaspersky Endpoint Security для Linux версии 12.2. Чтобы активировать функционал, необходимо:

- иметь действующую лицензию KUMA.
- использовать Kaspersky Security Center 14.2 и выше.
- использовать Kaspersky Endpoint Security для Linux 12.2 или выше.

Настройка получения событий состоит из следующих этапов:

1. Импорт нормализатора в KUMA.

   В KUMA должно быть настроено получение обновлений через серверы обновлений "Лаборатории Касперского".

   Нажмите Импорт ресурсов и выберите **[OOTB] KESL syslog cef** в списке доступных к установке нормализаторов.

2. Создание коллектора KUMA для получения событий Linux.

   Для получения событий Linux на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите нормализатор **[OOTB] KESL syslog cef**.

3. Запрос ключа в Службе технической поддержки.

   Если в вашей лицензии не было ключа активации функционала отправки журналов Linux в коллектор KUMA, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия KUMA и используется Kaspersky Endpoint Security для Linux версии 12.2. Мы планируем активировать функционал отправки журналов Linux в коллектор KUMA. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям KUMA не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено 2 ключа с лицензиями для KUMA и для активирования функционала Kaspersky Endpoint Security для Linux.

   В ответ на письмо вам будет предоставлен файл ключа.

4. Настройка на стороне Kaspersky Security Center и Kaspersky Endpoint Security для Linux.

   Файл ключа, активирующий функционал отправки событий Linux в коллекторы KUMA, необходимо импортировать в Kaspersky Security Center и распространить по конечным устройствам Kaspersky Security Center в соответствии с инструкцией. Также необходимо в политике Kaspersky Security Center добавить адреса серверов KUMA и настроить сетевые параметры подключения.

5. Проверка поступления событий Linux в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Linux выполнена правильно, в разделе веб-интерфейса KUMA Поиск связанных событий.

Kaspersky Endpoint Security для Linux передает следующие события:

- ProcessCreate
- ProcessTerminate
- FileChange
- New user account created
- User account deleted
- Group created
- Group deleted
- New member added to a group
- Member removed from the group
- User password changed
- Linux authentication performed
- Linux session started
- Linux session finished
- Service started
- Service stopped
- Promiscuous mode modified
- Audit configuration changed
- Account expiration date changed

Настройка получения событий Codemaster Mirada

Вы можете настроить получение событий Codemaster Mirada в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита системы Codemaster Mirada.
2. Создание коллектора KUMA для получения событий Codemaster Mirada.

   Для получения событий Codemaster Mirada в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Codemaster Mirada syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.
3. Установка коллектора в сетевой инфраструктуре KUMA.

4. Проверка поступления событий Codemaster Mirada в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Codemaster Mirada выполнена правильно, в разделе **События** веб-интерфейса KUMA.

Настройка аудита системы Codemaster Mirada

Система Codemaster Mirada может отправлять события по протоколу Syslog.

Чтобы настроить аудит событий в системе Codemaster Mirada:

1. Подключитесь к веб-интерфейсу системы Codemaster Mirada под учетной записью с правами администратора.
2. Перейдите в раздел **Настройки** → **Syslog**.
3. Включите сервис передачи событий, используя переключатель.
4. Выберите тип и формат протокола, нажав на кнопку со значком в виде точки, заключенной в круг.
5. В поле **Хост** укажите IP-адрес коллектора KUMA.
6. В поле **Протокол** укажите транспортный протокол **UDP** или **TCP**.
7. В поле **Порт** укажите порт, который прослушивает коллектор KUMA.

   По умолчанию используется порт 514.
8. В поле **Формат** укажите стандарт **RFC 3164**.
9. Нажмите на кнопку **Сохранить** в нижней части веб-интерфейса, чтобы сохранить внесенные изменения.

Настройка получения событий Postfix

Вы можете настроить получение событий системы Postfix в KUMA. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP. Ресурсы, описанные в этой статье, доступны для KUMA 3.0 и более новых версий.

Настройка получения событий состоит из следующих этапов:

1. Настройка Postfix для отправки событий.
2. Настройка коллектора KUMA для получения событий Postfix.
3. Проверка поступления событий Postfix в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Postfix выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Система Postfix формирует события в двух форматах:

- Многострочные события, содержащие информацию о сообщениях (с уникальным идентификатором). События имеют следующий вид:

<syslog PRI> время хост имя_процесса: идентификатор: информация из базового события 1

<syslog PRI> время хост имя_процесса: идентификатор: информация из базового события 2

- Однострочные, содержащие информацию об ошибках (без идентификатора). События имеют следующий вид:

  <syslog PRI> время хост имя_процесса: критичность: основная информация для парсинга

Для обработки событий системы Postfix используется набор ресурсов KUMA, который необходимо применить при создании коллектора:

- Нормализатор.
- Правило агрегации.
- Фильтры для точек назначения.

В процессе работы коллектора многострочные базовые события будут агрегированы на основе идентификатора событий, нормализованы, и одно событие будет направлено в хранилище и коррелятор.

Агрегированное событие примет следующий вид:

Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n

После агрегации полученное событие будет направлено в этот же коллектор, где будет выполняться нормализации агрегированного события.

Алгоритм обработки события системы Postfix

Для обработки события системы Postfix был реализован следующий алгоритм:

1. Первичная нормализация.

   На этом этапе выполняется первичная нормализация базовых событий, которые начинаются с символа "<", поступивших по syslog. События приводятся к формату, пригодному для последующей агрегации: из события выделяется первый символ и размещается в поле FlexString1, идентификатор размещается в поле ExternalID, имя хоста размещается в поле DeviceHostName. Базовая нормализация выполняется в основном нормализаторе.

2. Проверка на агрегацию.

   Выполняется проверка является ли событие агрегированным или нет. В результате проверки к неагрегированным событиям (первый символ не "{" и идентификатор не пустой) применяется правило агрегации, а затем агрегированные события направляются на повторную нормализацию.

3. Применение правила агрегации.

   На этом этапе к событиям применяется правило агрегации, базовые события "склеиваются" и принимают следующий вид:

   Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n.

4. После выполнения агрегации "склеенное" событие направляется обратно в этот же коллектор для выполнения нормализации агрегированного события.

   Чтобы замкнуть цикл обработки события, следует указать тот же самый коллектор в качестве точки назначения. На схеме точка назначения названа "Loop", чтобы обозначить цикл обработки события. Вы можете назвать точку назначения произвольным именем.

5. Нормализация агрегированного события.

   Нормализация агрегированного события. начинающегося с символа "{", выполняется в экстранормализаторах Aggregated events, Aggregated events. Message KV parser, Aggregated events. Message regex 1, Aggregated events. Message regex 2.

6. Отправка в хранилище и коррелятор.

   Агрегированные и нормализованные события отправляются в хранилище и коррелятор.

На следующем рисунке представлена схема обработки событий от системы Postfix.

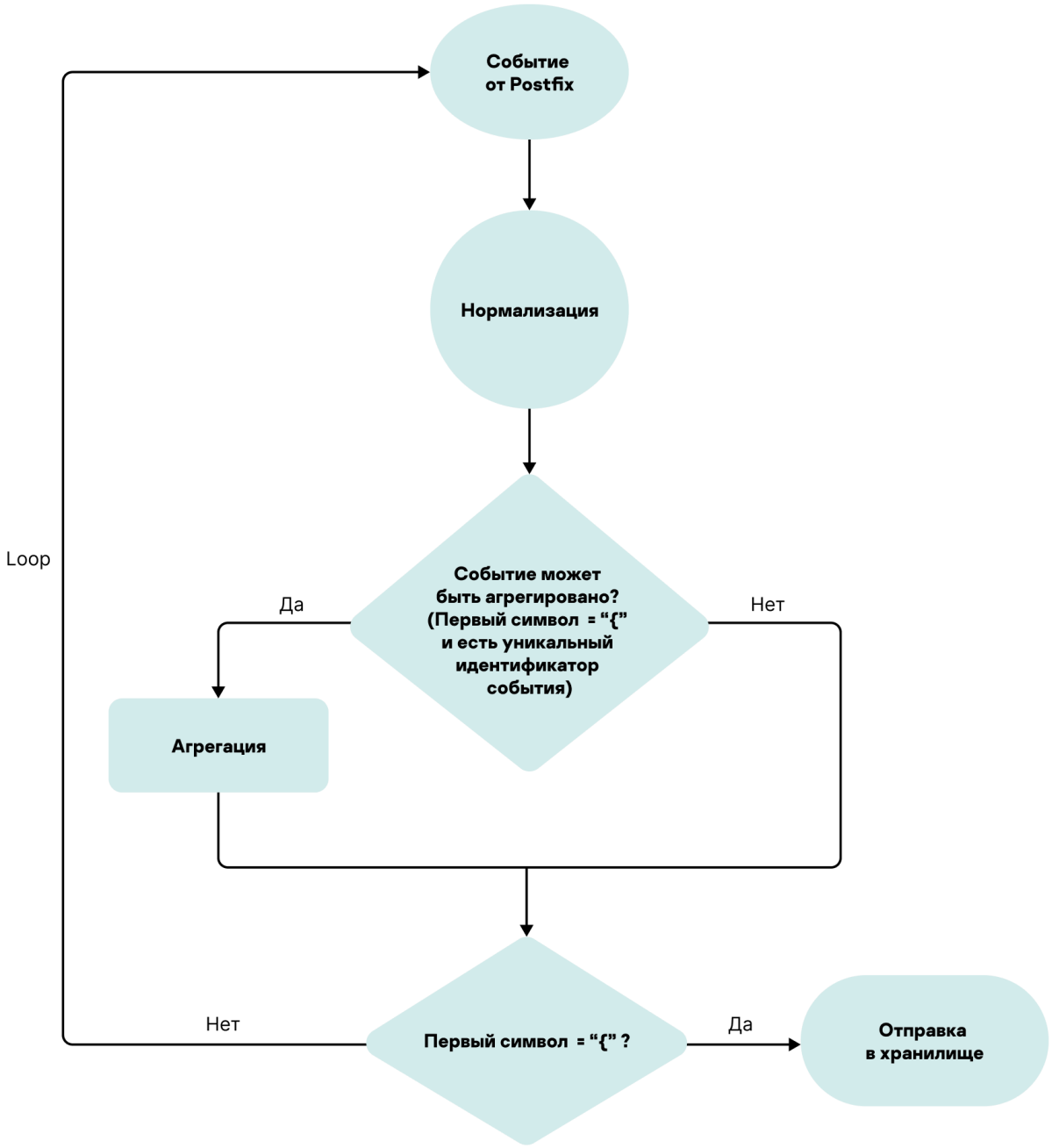


Схема обработки событий от системы Postfix

Настройка Postfix для отправки событий

События аудита системы Postfix по умолчанию направляются в файл /var/log/maillog или /var/log/mail.

Для отправки событий в KUMA:

1. Создайте резервную копию файла /etc/rsyslog.conf.

2. Откройте файл /etc/rsyslog.conf в режиме редактирования.

3. Добавьте в конец файла /etc/rsyslog.conf строку:

   ```
   mail.* @@<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
   ```

4. Сохраните файл /etc/rsyslog.conf

5. Перезапустите сервис rsyslog с помощью команды:

   ```
   sudo systemctl restart rsyslog
   ```

Настройка коллектора KUMA для получения и обработки событий Postfix

Чтобы настроить коллектор KUMA для получения событий Postfix:

1. Импортируйте пакет [OOTB] Postfix из репозитория KUMA. Пакет доступен для KUMA 3.0 и более новых версий.

2. Создайте новый коллектор и в мастере установки коллектора настройте следующие параметры:

   1. На шаге **Транспорт** в поле **Тип** выберите тип **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора.

   2. На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** в раскрывающемся списке **Нормализатор** выберите нормализатор **[OOTB] Postfix syslog**.

   3. На шаге **Агрегация событий** нажмите **Добавить правило агрегации** и в открывшемся окне **Агрегация событий** в раскрывающемся списке **Правило агрегации** выберите правило агрегации **[OOTB] Postfix. Aggreation rule**.

   4. На шаге **Маршрутизация** нажмите **Добавить** и в открывшемся окне **Создание точки назначения** последовательно создайте три точки назначения: этот же коллектор с именем `Loop`, хранилище и коррелятор.

      a. Создайте точку назначения с именем `Loop` со следующими параметрами:

      - На вкладке **Основные параметры** в раскрывающемся списке Тип выберите тип транспорта **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора, указанные ранее на шаге 2.1 этой инструкции.

      - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Filter for event aggregation**.

        Настройка этих параметров необходима для отправки агрегированного события в тот же самый коллектор для дальнейшей нормализации.

b. Создайте точку назначения коррелятора:

- На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **correlator** и заполните поле **URL**.
- На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Aggregated events to storage and correlator**.

c. Создайте точку назначения хранилища:

- На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **storage** и заполните поле **URL**.
- На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Aggregated events to storage and correlator**.

  Настройка этих параметров необходима для отправки агрегированного нормализованного события в хранилище и коррелятор.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора создан с заданными параметрами в веб-интерфейсе KUMA. На экране отобразится команда для установки сервиса на сервере.

4. Скопируйте команду установки коллектора и выполните команду установки коллектора на нужном сервере.

Коллектор настроен для получения и обработки событий Postfix.

Настройка получения событий CommuniGate Pro

Вы можете настроить получение событий системы CommuniGate Pro версий 6.1 и 6.5.1 в KUMA. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP. Ресурсы, описанные в этой статье, доступны для KUMA 3.0 и более новых версий. Поддерживается обработка части событий модуля SIP (события содержат последовательность символов "SIPDATA").

Настройка получения событий состоит из следующих этапов:

1. Настройка CommuniGate Pro для отправки событий.
2. Настройка коллектора KUMA для получения событий CommuniGate Pro.
3. Проверка поступления событий CommuniGate Pro в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий CommuniGate Pro выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Система CommuniGate Pro формирует событие аудита в виде нескольких отдельных записей, которые выглядят следующим образом:

```
<код события> временная отметка идентификатор направление: информация из базового события 1
```

```
<код события> временная отметка идентификатор направление: информация из базового события 2
```

```
<код события> временная отметка идентификатор направление: основная информация n
```

Для обработки событий системы CommuniGate Pro используется набор ресурсов KUMA, который необходимо применить при создании коллектора:

- Нормализатор.
- Правило агрегации.
- Фильтры для точек назначения.

В процессе работы коллектора многострочные базовые события будут агрегированы на основе идентификатора событий, нормализованы, и одно событие будет направлено в хранилище и коррелятор.

Агрегированное событие примет следующий вид:

```
Служебная информация из правила агрегации: идентификатор: информация из базового события
1, информация из базового события 2, информация из базового события n
```

После агрегации полученное событие будет направлено в этот же коллектор, где будет выполняться нормализация агрегированного события.

Алгоритм обработки события системы CommuniGate Pro

Для обработки события системы CommuniGate Pro был реализован следующий алгоритм:

1. Первичная нормализация.

   На этом этапе выполняется первичная нормализация базовых событий. Первым символом в базовом событии является число. События приводятся к формату, пригодному для последующей агрегации: из события выделяется первый символ и размещается в поле DeviceCustomString1, идентификатор размещается в поле ExternalID, имя хоста размещается в поле DeviceHostName. Базовая нормализация выполняется в основном нормализаторе.

2. Проверка на агрегацию.

   Выполняется проверка, является ли событие агрегированным. В результате проверки к неагрегированным событиям (первый символ события является числом) применяется правило агрегации, а затемагрегированные события направляются на повторную нормализацию. Агрегация выполняется с помощью правила **[OOTB] CommuniGate Pro. Aggregation rule**.

3. Применение правила агрегации.

   На этом этапе к событиям применяется правило агрегации, базовые события "склеиваются" и принимают следующий вид:

   Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n.

   После выполнения агрегации "склеенное" событие направляется обратно в этот же коллектор для выполнения нормализации агрегированного события.

   Чтобы замкнуть цикл обработки события, следует указать тот же самый коллектор в качестве точки назначения. На схеме точка назначения названа "Loop", чтобы обозначить цикл обработки события. Вы можете назвать точку назначения произвольным именем.

4. Нормализация агрегированного события.

   Нормализация агрегированного события. начинающегося с символа "{", выполняется в экстранормализаторах Aggregated events, Aggregated events - kv part.

5. Отправка в хранилище и коррелятор.

   Агрегированные и нормализованные события отправляются в хранилище и коррелятор.

На следующем рисунке представлена схема обработки событий от системы CommuniGate Pro.

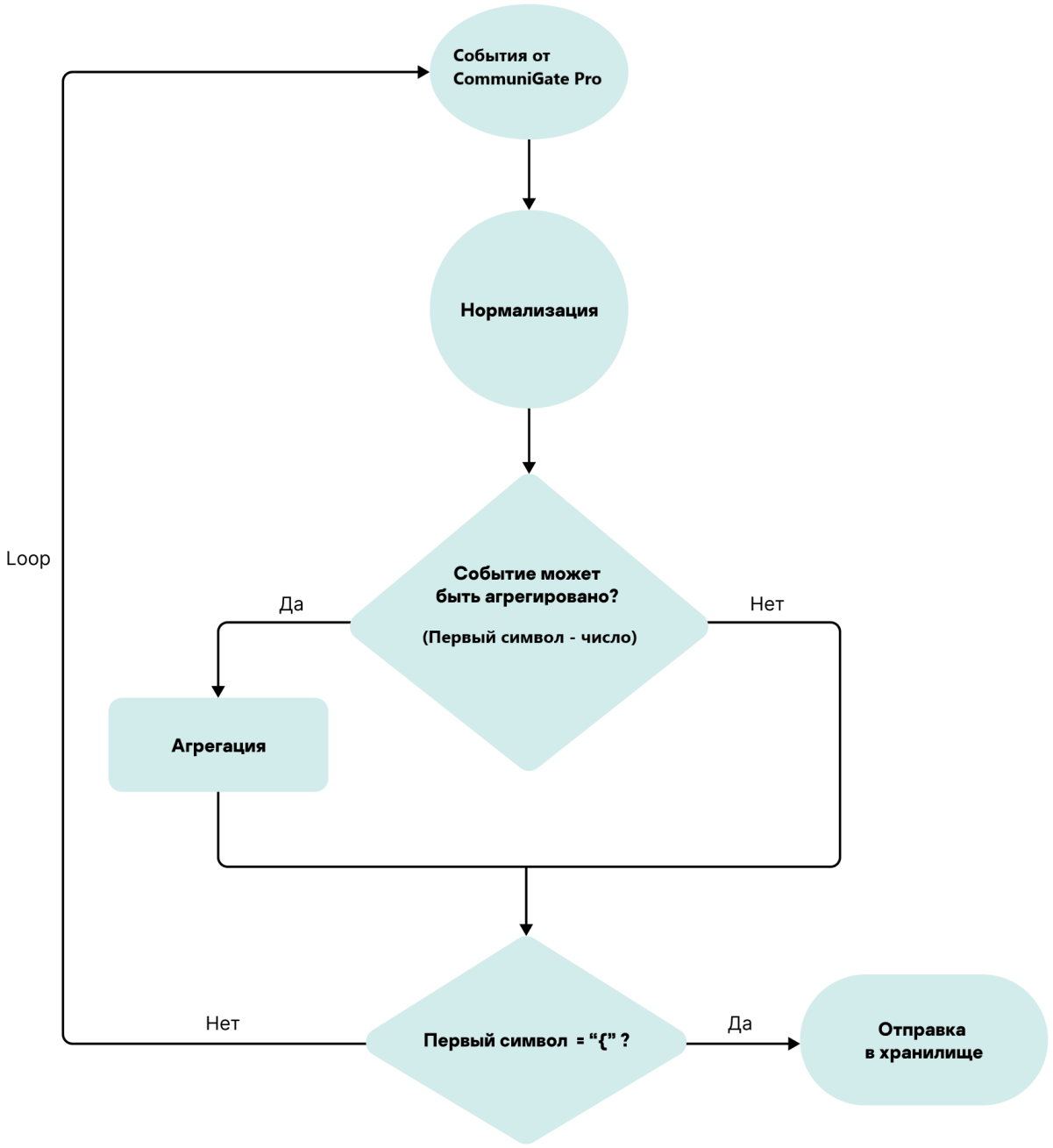


Схема обработки событий от системы CommuniGate Pro

Настройка CommuniGate Pro для отправки событий

События аудита системы CommuniGate Pro по умолчанию направляются в директорию /var/CommuniGate/SystemLogs/ в файлы журналов с расширением .log.

Для отправки событий в KUMA необходимо установить на сервер CommuniGate Pro агент KUMA и настроить чтение файлов с расширением .log из директории /var/CommuniGate/SystemLogs/ и отправку по протоколу TCP в коллектор KUMA.

Чтобы создать агент, который будет выполнять чтение и передачу в KUMA событий:

1. В веб-консоли KUMA перейдите в раздел **Ресурсы и сервисы** → **Агенты** и нажмите **Добавить**.

2. В открывшемся окне **Создание агента** на вкладке **Основные параметры** в поле **Название** укажите название агента.

3. На вкладке **Подключение №1** заполните следующие поля:

   a. В блоке параметров **Коннектор** на вкладке **Основные параметры** задайте следующие значения для коннектора:

      1. В поле **Название** укажите название, например, `CommuniGate file`.

      2. В раскрывающемся списке **Тип** выберите значение **file**.

      3. В поле **Путь к файлу** укажите значение:

         /var/CommuniGate/SystemLogs/.*.log

   b. В блоке параметров **Точки назначения** на вкладке **Основные параметры** задайте следующие значения для точки назначения:

      1. В поле **Название** укажите название, например, `CommuniGate TCP collector`.

      2. В раскрывающемся списке **Тип** выберите значение **tcp**.

      3. В поле **URL** укажите FQDN или IP-адрес и порт коллектора KUMA.

4. Нажмите на кнопку **Создать**.

5. После того как сервис агента создан в KUMA, следует установить агент на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

Настройка коллектора KUMA для получения и обработки событий CommuniGate Pro

Чтобы настроить коллектор KUMA для получения событий CommuniGate Pro:

1. Импортируйте пакет [OOTB] CommuniGate Pro из репозитория KUMA. Пакет доступен для KUMA 3.0 и более новых версий.

2. Создайте новый коллектор и в мастере установки коллектора настройте следующие параметры:

   1. На шаге **Транспорт** в поле **Тип** выберите тип **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора.

   2. На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** в раскрывающемся списке **Нормализатор** выберите нормализатор **[OOTB] CommuniGate Pro**.

   3. На шаге **Агрегация событий** нажмите **Добавить правило агрегации** и в открывшемся окне **Агрегация событий** в раскрывающемся списке **Правило агрегации** выберите правило агрегации **[OOTB] CommuniGate Pro. Aggreation rule**.

4. На шаге **Маршрутизация** нажмите **Добавить** и в открывшемся окне **Создание точки назначения** последовательно создайте три точки назначения: этот же коллектор с именем `Loop`, хранилище и коррелятор:

   a. Создайте точку назначения с именем `Loop` со следующими параметрами:

      - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите тип транспорта **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора, указанные ранее на шаге 2.1 этой инструкции.

      - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Filter for event aggregation**.

      Настройка этих параметров необходима для отправки агрегированного события в тот же самый коллектор для дальнейшей нормализации.

   b. Создайте точку назначения коррелятора:

      - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **correlator** и заполните поле **URL**.

      - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

   c. Создайте точку назначения хранилища:

      - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **storage** и заполните поле **URL**.

      - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

      Настройка этих параметров необходима для отправки агрегированного нормализованного события в хранилище и коррелятор.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора создан с заданными параметрами в веб-интерфейсе KUMA. На экране отобразится команда для установки сервиса на сервере.

4. Скопируйте команду установки коллектора и выполните команду установки коллектора на нужном сервере.

Коллектор настроен для получения и обработки событий CommuniGate Pro.

Настройка получения событий Yandex Cloud

Вы можете настроить получение событий системы Yandex Cloud в KUMA. Нормализатор поддерживает обработку событий аудита уровня конфигурации, хранящихся в файлах с расширением .json.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий Yandex Cloud.

2. Настройка передачи событий Yandex Cloud.

3. Настройка коллектора KUMA для получения и обработки событий Yandex Cloud.

   Для получения событий Yandex Cloud в мастере установки коллектора KUMA необходимо выполнить следующие действия:

   1. В мастере установки коллектора KUMA на шаге **Транспорт** выберите коннектор типа **file**.
   2. В поле **URL** укажите `/var/log/yandex-cloud/<audit_trail_id>/*/*/*/*.json`, где <audit_trail_id> - идентификатор аудита.
   3. На шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Yandex Cloud**.

4. Установка коллектора в сетевой инфраструктуре KUMA.

5. Проверка поступления событий Yandex Cloud в коллектор KUMA.

   Чтобы проверить, что настройка сервера источника событий Yandex Cloud выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка аудита событий Yandex Cloud

Настройка передачи событий включает следующие шаги:

1. Подготовка среды для работы с Yandex Cloud.
2. Создание бакета для аудитных логов.
3. Создание ключа шифрования в сервисе Key Management Service.
4. Включение шифрования бакета.
5. Создание сервисных аккаунтов.
6. Создание статического ключа.
7. Назначение роли сервисным аккаунтам.
8. Создание аудит трейла.

Подготовка среды для работы с Yandex Cloud

Для выполнения работ по настройке необходим Yandex Cloud CLI, установите и инициализируйте его.

Примечание: по умолчанию аудит будет осуществляться в каталоге Yandex Cloud, указанном в профиле CLI. Вы можете указать другой каталог с помощью параметра `--folder-name` или `--folder-id`.

Для настройки аудита необходим активный платежный аккаунт, поскольку за использование инфраструктуры Yandex Cloud взимается плата.

Чтобы настроить аудит Yandex Cloud, требуется активный платежный аккаунт:

1. Перейдите в консоль управления, затем войдите в Yandex Cloud или зарегистрируйтесь.

2. На странице Yandex Cloud Billing убедитесь, что у вас подключен платежный аккаунт, и он находится в статусе ACTIVE или TRIAL_ACTIVE. Если платежного аккаунта нет, создайте его.

Если у вас есть активный платежный аккаунт, вы можете создать или выбрать каталог Yandex Cloud, в котором будет работать ваша инфраструктура, на странице облака.

Создание бакета для аудитных логов

Чтобы создать бакет:

1. В консоли управления перейдите в каталог, в котором хотите создать бакет, например, **example-folder**.

2. Выберите сервис **Object Storage**.

3. Нажмите **Создать бакет**.

4. На странице создания бакета выполните следующие действия:

   1. Введите имя бакета в соответствии с правилами именования, например, **kumabucket**.

   2. При необходимости ограничьте максимальный размер бакета. Размер 0 означает отсутствие ограничений и аналогичен включенной опции **Без ограничения**.

   3. Выберите тип доступа **Ограниченный**.

   4. Выберите класс хранилища по умолчанию.

   5. Нажмите **Создать бакет**.

Бакет создан.

Создание ключа шифрования в сервисе Key Management Service

Чтобы создать ключ шифрования:

1. В консоли управления перейдите в каталог **example-folder**.

2. Выберите сервис **Key Management Service**.

3. Нажмите **Создать ключ** и укажите следующие параметры:

   - Имя – например, **kuma-kms**.
   - Алгоритм шифрования – **AES-256**.
   - Для остальных параметров оставьте значения по умолчанию.

4. Нажмите **Создать**.

   Ключ шифрования создан.

Включение шифрования бакета

Чтобы включить шифрование бакета:

1. В консоли управления перейдите в бакет, созданный ранее.
2. На панели слева выберите **Шифрование**.
3. В поле **Ключ KMS** выберите ключ **kuma-kms**.
4. Нажмите **Сохранить**.

   Шифрование бакета включено.

Создание сервисных аккаунтов

Чтобы создать сервисные аккаунты – отдельный аккаунт для трейла и отдельный аккаунт бакета, выполните следующие шаги:

1. Создайте сервисный аккаунт **sa-kuma**:

   1. В консоли управления перейдите в каталог **example-folder**.
   2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.
   3. Нажмите **Создать сервисный аккаунт** и введите имя сервисного аккаунта, например **sa-kuma**, в соответствии с правилами именования:

      - длина – от 3 до 63 символов;
      - может содержать строчные буквы латинского алфавита, цифры и дефисы;
      - первый символ – буква, последний – не дефис.

   4. Нажмите **Создать**.

2. Создайте сервисный аккаунт **sa-kuma-bucket**:

    1. В консоли управления перейдите в каталог **example-folder**.

    2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.

    3. Нажмите **Создать сервисный аккаунт** и введите имя сервисного аккаунта, например **sa-kuma-bucket**, в соответствии с правилами именования:

        - длина – от 3 до 63 символов;

        - может содержать строчные буквы латинского алфавита, цифры и дефисы;

        - первый символ – буква, последний – не дефис.

    4. Нажмите **Создать**.

    Сервисные аккаунты созданы.

Создание статического ключа

Идентификатор ключа и секретный ключ понадобятся на этапе монтирования бакета. Ключ можно создать с помощью консоли управления или с помощью CLI.

Чтобы создать ключ с помощью консоли управления:

1. В консоли управления перейдите в каталог **example-folder**.

2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.

3. Выберите сервисный аккаунт **sa-kuma-bucket** и нажмите на строку с его именем.

4. На верхней панели нажмите **Создать новый ключ**.

5. Выберите **Создать статический ключ доступа**.

6. Задайте описание ключа и нажмите **Создать**.

7. Сохраните идентификатор и секретный ключ.

Статический ключ доступа создан. После закрытия диалога значение ключа будет недоступно.

Чтобы создать ключ с помощью CLI:

1. Создайте ключ доступа для сервисного аккаунта **sa-kuma-bucket**:

    ```
    yc iam access-key create --service-account-name sa-kuma-bucket
    ```

    Результат: `ls`

    ```
    access_key:
    id: aje*******k2u
    service_account_id: aje*******usm
    ```

```
created_at: "2022-09-22T14:37:51Z"
key_id: 0n8*******0YQ
secret: JyT*******zMP1
```

2. Сохраните идентификатор key_id и секретный ключ secret. Получить значение ключа повторно будет невозможно.

Ключ доступа создан.

Назначение ролей сервисным аккаунтам

Чтобы назначить сервисному аккаунту sa-kuma роли audit-trails.viewer, storage.uploader и kms.keys.encrypterDecrypter:

1. В CLI назначьте роль audit-trails.viewer на каталог:

```
yc resource-manager folder add-access-binding \
--role audit-trails.viewer \
--id <идентификатор_каталога> \
--service-account-id <идентификатор_сервисного_аккаунта>
```

Где:

- `--role` – назначаемая роль;
- `--id` – идентификатор каталога example-folder;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

2. Назначьте роль storage.uploader на каталог с бакетом:

```
yc resource-manager folder add-access-binding \
--role storage.uploader \
--id <идентификатор_каталога> \
--service-account-id <идентификатор_сервисного_аккаунта>
```

Где:

- `--role` – назначаемая роль;
- `--id` – идентификатор каталога example-folder;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

3. Назначьте роль kms.keys.encrypterDecrypter на ключ шифрования kuma-kms:

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <идентификатор_ключа> \
--service-account-id <идентификатор_сервисного_аккаунта>
```

Где:

- `--role` – назначаемая роль;
- `--id` – идентификатор KMS-ключа kuma-kms;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

Чтобы назначить сервисному аккаунту sa-kuma-bucket роли storage.viewer и kms.keys.encrypterDecrypter:

1. В CLI назначьте роль storage.viewer на каталог:
   ```
   yc resource-manager folder add-access-binding \
   --id <идентификатор_каталога> \
   --role storage.viewer \
   --service-account-id <идентификатор_сервисного_аккаунта>
   ```
   Где:
   - `--id` – идентификатор каталога example-folder;
   - `--role` – назначаемая роль;
   - `--service-account-id` – идентификатор сервисного аккаунта sa-kuma-bucket.
2. Назначьте роль kms.keys.encrypterDecrypter на ключ шифрования kuma-kms:
   ```
   yc kms symmetric-key add-access-binding \
   --role kms.keys.encrypterDecrypter \
   --id <идентификатор_ключа> \
   --service-account-id <идентификатор_сервисного_аккаунта>
   ```
   Где:
   - `--role` – назначаемая роль;
   - `--id` – идентификатор KMS-ключа kuma-kms;
   - `--service-account-id` – идентификатор сервисного аккаунта sa-kuma-bucket.

Создание аудит трейла

Чтобы создать аудит трейл:

1. В консоли управления перейдите в каталог **example-folder**.
2. Выберите сервис **Audit Trails**.
3. Нажмите **Создать трейл** и укажите имя создаваемого трейла, например, **kuma-trail**.

4. В блоке **Назначение** задайте параметры объекта назначения:

   - **Назначение** – **Object Storage**.
   - **Бакет** – имя бакета, например, **kumabucket**.
   - **Префикс объекта** – необязательный параметр, участвует в полном имени файла аудитного лога.

     Используйте префикс, если вы храните аудитные логи и сторонние данные в одном и том же бакете. Не используйте одинаковый префикс для логов и других объектов в бакете, так как в этом случае логи и сторонние объекты могут перезаписать друг друга.
   - **Ключ шифрования** – укажите ключ шифрования kuma-kms, которым зашифрован бакет.

5. В блоке **Сервисный аккаунт** выберите **sa-kuma**.

6. В блоке **Сбор событий с уровня конфигурации** задайте параметры сбора аудитных логов уровня конфигурации:

   - **Сбор событий** – выберите **Включено**.
   - **Ресурс** – выберите **Каталог**.
   - **Каталог** – не требует заполнения, содержит имя текущего каталога.

7. В блоке **Сбор событий с уровня сервисов** в поле **Сбор событий** выберите **Выключено**.

8. Нажмите **Создать**.

Настройка передачи событий Yandex Cloud

Бакет необходимо смонтировать на сервере, на котором будет установлен коллектор KUMA.

Чтобы смонтировать бакет:

1. На сервере создайте директорию для пользователя kuma:

   ```
   sudo mkdir /home/kuma
   ```

2. На сервере создайте файл со статическим ключом доступа сервисного аккаунта sa-kuma-bucket и предоставьте на него права пользователю kuma:

   ```
   sudo bash -c 'echo <идентификатор_ключа_доступа>:<секретный_ключ_доступа> >
   /home/kuma/.passwd-s3fs'
   sudo chmod 600 /home/kuma/.passwd-s3fs
   sudo chown -R kuma:kuma /home/kuma
   ```

3. Установите пакет s3fs:

   ```
   sudo apt install s3fs
   ```

4. Создайте каталог, в который будет монтироваться бакет, и предоставьте на него права пользователю kuma:

   ```
   sudo mkdir /var/log/yandex-cloud/
   sudo chown kuma:kuma /var/log/yandex-cloud/
   ```

5. Смонтируйте бакет:

   ```
   sudo s3fs kumabucket /var/log/yandex-cloud -o passwd_file=/home/kuma/.passwd-s3fs -o
   url=https://storage.yandexcloud.net -o use_path_request_style -o uid=$(id -u kuma) -o
   gid=$(id -g kuma)
   ```

   Вы можете настроить монтирование бакета при запуске операционной системы, для этого добавьте в файл /etc/fstab строку вида:

   ```
   s3fs#kumabucket /var/log/yandex-cloud fuse _netdev,uid=<kuma_uid>,gid=
   <kuma_gid>,use_path_request_style,url=https://storage.yandexcloud.net,passwd_file=/home
   s3fs 0 0
   ```

   Где:

   <kuma_uid> – идентификатор пользователя kuma в операционной системе.

   <kuma_gid> – идентификатор группы пользователей kuma в операционной системе.

   Чтобы узнать kuma_uid и kuma_gid, в консоли выполните команду:

   ```
   id kuma
   ```

6. Проверьте, что бакет смонтирован:

   ```
   sudo ls /var/log/yandex-cloud/
   ```

   Если все настроено верно, команда вернет <audit_trail_id>, где <audit_trail_id> – идентификатор трейла аудита.

Настройка передачи событий Yandex Cloud завершена. События будут располагаться в каталогах в файлах с расширением .json:

/var/log/yandex-cloud/{audit_trail_id}/{year}/{month}/{day}/*.json

Настройка получения событий Microsoft 365

Вы можете настроить получение событий из облачного решения Microsoft 365 (Office 365) в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка доступа к интерфейсам API управления Office 365 стандартными методами Microsoft

   Для получения событий в KUMA выдайте необходимый набор разрешений API:

   Microsoft.Graph

   Directory.Read.All

   API управления Office 365

   ActivityFeed.Read

   ActivityFeed.Read.Dlp

2. Создание коллектора KUMA

   Для получения событий Microsoft 365 создайте коллектор со следующими параметрами:

   - На шаге **Транспорт** укажите тип коннектора **office365**.
   - На шаге **Парсинг событий** укажите нормализатор **[OOTB] Microsoft Office 365 json**.

3. Установка коллектора в сетевой инфраструктуре KUMA

4. Проверка поступления событий Microsoft 365 в коллектор KUMA

   Чтобы проверить, что настройка сервера источника событий Microsoft 365 выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка получения событий АПКШ Континент

В поставку KUMA входит утилита kuma-kont, которая состоит из исполняемого файла и файла конфигурации. Поддерживается работа под управлением операционных систем Astra Linux, Ubuntu 22.04 LTS и РЕД ОС 7.3.4 и 8. Утилита позволяет выполнить подключение к базе данных MSSQL, получать события АПКШ Континент и отправлять данные в коллектор KUMA в формате JSON. Импорт данных поддерживается для АПКШ Континент 3.9.2.

Настройка сбора из базы данных MSSQL событий АПКШ Континент и их отправка в коллектор KUMA состоит из следующих этапов:

1. Подготовительные действия для получения событий АПКШ Континент.

   На данном этапе необходимо создать коллектор KUMA, который будут осуществлять прием событий, а также создать пользователя в базе данных MSSQL.

2. Настройка утилиты kuma-kont.

   На данном этапе необходимо создать конфигурационный файл утилиты и сервис утилиты.

3. Запуск утилиты kuma-kont.

   После активации утилита начнет выполнять экспорт событий из БД MSSQL и отправку в коллектор KUMA. Доступен журнал kuma-kont.log.

Подготовительные действия для получения событий АПКШ Континент

1. Создание коллектора KUMA.

   1. Создание коллектора KUMA для событий АПКШ Континент 3.9.

      Для получения событий аудита системы Континент 3.9 с помощью мастера установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] SecurityCode Continent 3.9 json**. Также на вкладке **Транспорт** требуется задать порт и протокол, указанные в конфигурационном файле kuma-kont-config.yaml в группе параметров KUMA Collector.

   2. Установка коллектора в сетевой инфраструктуре KUMA.

2. Создание учетной записи в СУБД MS SQL.

   Создайте учетную запись в базе данных с минимально необходимым набором прав для подключения и чтения данных в таблицах: ALERTLOG, SERVERACCESSLOG, SYSTEMLOG, PACKETLOG, FILTERS.

3. Обеспечение сетевой связанности.

   Необходимо обеспечить сетевую связанность между сервером, на котором работает утилита и сервером БД системы Континент, а также между сервером, на котором работает утилита и сервером коллектора KUMA.

Настройка утилиты kuma-kont

Настройка утилиты kuma-kont состоит из следующих этапов:

1. Создание конфигурационного файла kuma-kont-config.yaml.
2. Создание сервиса kuma-kont.

Создание конфигурационного файла kuma-kont-config.yaml

Чтобы создать конфигурационный файл kuma-kont-config.yaml:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer/roles/kuma/files
   ```

2. Распакуйте архив kuma-kont.tar:

   ```
   tar -xvf kuma-kont.tar
   ```

3. Перейдите в директорию с утилитой:

   ```
   cd kuma-kont
   ```

4. Скопируйте шаблон kuma-kont-config-template.yaml и создайте конфигурационный файл с именем kuma-kont-config.yaml:

   ```
   cp kuma-kont-config-template.yaml kuma-kont-config.yaml
   ```

5. Измените права на чтения для файла конфигурации:

   ```
   sudo chown <учетная запись>:<учетная запись> kuma-kont-config.yaml
   sudo chmod 600 kuma-kont-config.yaml
   ```

   Замените <учетная запись> на имя пользователя операционной системы, от которого будет запускаться сервис.

6. Отредактируйте параметры конфигурационного файла kuma-kont-config.yaml.

   Необходимо задать значения для следующих параметров:

   - параметры группы General settings: state_file, log_file_path.
   - параметры группы Kontinent Database: name, user, password, host, port.
   - параметры группы KUMA Collector: address, port, protocol.

     Пример настройки параметров приведен в файле kuma-kont-config-template.yaml.

7. Сохраните изменения в файле.

Конфигурационный файл создан.

Создание сервиса

Чтобы создать сервис kuma-kont:

1. Измените права на запуск для исполняемого файла:

   ```
   sudo chown <учетная запись>:<учетная запись> <путь к исполняемому файлу>
   sudo chmod 700 <путь к исполняемому файлу>
   ```

2. Создайте файл с именем `kuma-kont.service` в директории /etc/systemd/system/ со следующим содержимым:

   ```
   [Unit]
   Description=Connector Kontinent 3.9
   After=network.target
   [Service]
   User=<учетная запись>
   ExecStart=<путь к исполняемому файлу> --config <путь к файлу конфигурации>
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

   Замените <учетная запись> на имя пользователя операционной системы, от которого будет запускаться сервис.

3. Укажите путь к исполняемому файлу

   Укажите путь к исполняемому файлу `kuma-kont ` в поле `ExecStart`.

   Например, если файл `kuma-kont` находится в директории `/usr/bin/`, то оставьте значение по умолчанию.

4. Укажите путь к конфигурационному файлу

   Укажите путь к конфигурационному файлу `kuma-kont-config.yaml` в поле `ExecStart`. Например, если файл `kuma-kont-config.yaml` находится в директории `/path/to/`, то укажите этот путь.

   Пример файла `kuma-kont.service`

   ```
   [Unit]
   Description=Continent Service
   After=network.target
   [Service]
   User=user-example
   ExecStart=./usr/bin/kuma-kont --config /path/to/kuma-kont-config.yaml
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

5. Загрузите конфигурацию менеджера systemd, выполнив команду:

   ```
   sudo systemctl daemon-reload
   ```

6. Добавьте сервис в автозагрузку операционной системы, выполнив команду:

   ```
   sudo systemctl enable kuma-kont
   ```

Теперь утилита kuma-kont будет запускаться как сервис при загрузке системы.

Запуск и управление сервисом утилиты kuma-kont

Для запуска сервиса утилиты выполните команду:

```
sudo systemctl start kuma-kont
```

Будет начат сбор событий из базы данных MSSQL и их отправка в коллектор KUMA.

Управление сервисом утилиты осуществляется с помощью следующих команд:

1. Запуск сервиса kuma-kont:

   ```
   sudo systemctl start kuma-kont
   ```

2. Остановка сервиса kuma-kont:

   ```
   sudo systemctl stop kuma-kont
   ```

3. Перезапуск сервиса kuma-kont:

   ```
   sudo systemctl restart kuma-kont
   ```

Также можно выполнить отправку событий с помощью утилиты kuma-kont, работающей как приложение. Чтобы начать отправку событий в коллектор KUMA необходимо выполнить следующую команду, находясь в директории с исполняемым файлом:

```
./kuma-kont --config <путь к файлу kuma-kont-config.yaml>
```

Поведение при потере соединения

Соединение с базой данных MSSQL.

При потере соединения с базой данных MSSQL утилита будет пытаться восстановить соединение с ним каждые n секунд (где n – равно значению параметра poll_interval, конфигурационного файла), до тех пор, пока соединение не будет восстановлено.

Соединение с коллектором KUMA.

В случае использования протокола TCP для отправки событий при потере соединения с коллектором KUMA утилита также будет пытаться его восстановить. Интервал между попытками установить соединение будет увеличиваться до тех пор, пока не достигнет одного часа, затем попытка установить соединение будет выполняться один раз в час.

Известные ограничения

Не полностью расшифровывается событие из таблицы `AlertLog` со значением "AL_CATEGORY" = 5.

Параметры конфигурационного файла kuma-kont-config.yaml

В таблице представлены параметры, доступные для настройки в файле kuma-kont-config.yaml.

Параметры конфигурационного файла kuma-kont-config.yaml

Параметр	Описание
`debug`	Необязательный параметр в группе **General settings**. Используется при необходимости вывода логов уровня отладки. При значении false, выводятся только сообщения о старте и завершении работы, а также ошибки, которые возникли в процессе отправки. Доступные значения: • **true** • **false** Значение по умолчанию: **false**.
`need_reconnect`	Необязательный параметр в группе **General settings**. Параметр определяет будет ли утилита выполнять переподключение к базе данных при каждом запросе. Доступные значения: • **true** • **false** Значение по умолчанию: **false**.
`state_file`	Обязательный параметр в группе **General settings**. Абсолютный путь к JSON-файлу, который используется для сохранения состояния обработанных логов. Файл создается автоматически по данному адресу. Убедитесь, что у пользователя достаточно прав на запись в эту директорию. Пример: /home/user/kuma-kont/state.json
`log_file_path`	Обязательный параметр в группе **General settings**. Абсолютный путь к файлу журналов для записи действий коннектора. Файл создается автоматически по данному адресу. Убедитесь, что у пользователя достаточно прав на запись в эту директорию. Пример: /home/user/kuma-kont/kuma-kont.log
`poll_interval`	Необязательный параметр в группе **General settings**. Интервал опроса базы данных. По умолчанию: 10 секунд При высоком потоке EPS мы не рекомендуем указывать значение выше 15 секунд.
`name`	Обязательный параметр в группе **Kontinent Database**. Названия базы данных, в которую приходят журналы АПКШ.
`user`	Обязательный параметр в группе **Kontinent Database**. Имя пользователя базы данных.
`password`	Обязательный параметр в группе **Kontinent Database**. Пароль пользователя базы данных.
`host`	Обязательный параметр в группе **Kontinent Database**. URL сервера базы данных.
`port`	Обязательный параметр в группе **Kontinent Database**. Порт сервера базы данных. Убедитесь, что он доступен с сервера, на котором установлена утилита.
`limit`	Необязательный параметр в группе **Kontinent Database**. Ограничение по количеству выгружаемых событий из базы данных за один раз. По умолчанию 100_000 событий за один опрос базы данных. Мы не рекомендуем указывать меньшее значение при высоком потоке EPS.

Параметр	Описание
`alert_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа AlertLog, с которого необходимо начать отправлять события в коллектор KUMA. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`packet_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа PacketLog, с которого необходимо начать отправлять события в коллектор KUMA. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`server_access_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа ServerAccessLog, с которого необходимо начать отправлять события в коллектор KUMA. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`system_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа SystemLog, с которого необходимо начать отправлять события в коллектор KUMA. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`address`	Обязательный параметр в группе **KUMA Collector**. Полное доменное имя (FQDN) или IP-адрес сервера, на котором установлен коллектор KUMA.
`port`	Обязательный параметр в группе **KUMA Collector**. Порт коллектора KUMA.
`protocol`	Обязательный параметр в группе **KUMA Collector**. Протокол передачи данных, который используется в коллекторе KUMA. Если используется протокол udp, повторная отправка событий при потере соединения с коллектором KUMA не будет осуществлена. Доступные значения: • **tcp** • **udp**

Настройка получения событий VK WorkSpace Mail

KUMA позволяет осуществлять мониторинг событий системы VK WorkSpace Mail версии 1.23, поступающих в формате syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка отправки событий VK WorkSpace Mail.

2. Создание коллектора KUMA для событий VK WorkSpace Mail.

   Для получения событий аудита системы VK WorkSpace Mail с помощью мастера установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] VK WorkSpace Mail syslog**. Также на вкладке **Транспорт** требуется указать порт и протокол в соответствии с пунктами 2.2, 2.3 инструкции *Настройка отправки событий VK WorkSpace Mail*.

3. Установка коллектора в сетевой инфраструктуре KUMA.

4. Проверка поступления событий VK WorkSpace Mail в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий VK WorkSpace Mail выполнена правильно в разделе веб-интерфейса KUMA Поиск связанных событий.

Настройка отправки событий VK WorkSpace Mail

Для настройки передачи событий в KUMA выполните следующие действия:

1. Перейдите в меню **Настройки дублирования действий пользователей во внешние хранилища**.
2. Установите флажок для параметра **Дублировать действия пользователей в syslog**.
   a. В поле **Адрес сервера syslog** укажите IP-адрес или FQDN коллектора KUMA.
   b. В поле **Порт сервера syslog** укажите порт, который прослушивает коллектор KUMA.
   c. В поле **Протокол syslog, TCP или UDP** выберите протокол передачи данных.
   d. В поле **Идентификатор данных syslog** укажите bein.

Настройка отправки событий VK WorkSpace Mail выполнена.

Настройка получения событий Angie

KUMA позволяет осуществлять мониторинг событий аудита веб-сервера Angie или Angie Pro (версии 1.10.1 и выше), развернутого на устройствах под управлением операционных систем семейства Linux.

Настройка передачи и получения событий состоит из следующих этапов:

1. Настройка передачи событий Angie
2. Создание коллектора KUMA для событий Angie

   Для получения событий в мастере установки коллектора KUMA на шаге **Парсинг событий** выберите нормализатор **[OOTB] Angie syslog**.
3. Установка коллектора в сетевой инфраструктуре KUMA
4. **Проверка поступления событий Angie в коллектор KUMA**

   Вы можете проверить, что настройка поступления событий из Angie и Angie Pro выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка передачи событий Angie

Чтобы настроить параметры передачи событий Angie:

1. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду:
   ```
   sudo angie -t
   ```

   Возможные сообщения при проверке конфигурационного файла

   Если в конфигурационном файле синтаксические ошибки отсутствуют, Angie отобразит уведомления:

   ```
   angie: the configuration file /etc/angie/angie.conf syntax is ok
   ```

```
angie: configuration file /etc/angie/angie.conf test is successful
```

Если в конфигурационном файле найдены синтаксические ошибки, Angie сообщит, в чем заключается ошибка, например:

```
angie: [emerg] "http" directive is not allowed here in etc/angie/http.d/angie-to-siem.conf:1
angie: configuration file /etc/angie/angie.conf test failed
```

Подробнее о синтаксисе конфигурационного файла см. в официальной документации Angie.

2. Если проверка синтаксиса прошла успешно (получен результат `test is successful`), выполните резервное копирование исходного конфигурационного файла с помощью следующей команды:
   ```
   sudo cp /etc/angie/angie.conf /etc/angie/angie_backup.conf
   ```

3. Откройте конфигурационный файл *angie.conf*, выполнив следующую команду:
   ```
   sudo vi /etc/angie/angie.conf
   ```

   Стандартный конфигурационный файл angie.conf по умолчанию располагается в директории `/etc/angie`.

   Если в работе веб-сервера Angie используется нестандартный конфигурационный файл, необходимо открыть именно его. Вы можете узнать текущее расположение этого файла с помощью следующей команды:

   ```
   sudo angie -V
   ```

   Расположение файла указано в параметре `--config-path`.

4. Проверьте, что в контексте `http` указана директива `include`, которая разрешает управление конфигурацией с помощью дочерних конфигурационных файлов, выполнив следующую команду:
   ```
   include /etc/angie/http.d/*.conf
   ```

5. Создайте конфигурационный файл angie-to-siem.conf в директории `/etc/angie/http.d/` с помощью следующей команды:
   ```
   touch /etc/angie/http.d/angie-to-siem.conf
   ```

6. Откройте конфигурационный файл angie-to-siem.conf, с помощью команды `sudo vi /etc/angie/http.d/angie-to-siem.conf`.

7. В директиве `log_format` укажите формат отправляемых событий следующим образом:
   ```
   log_format syslog
   device_event_category=access_log|time=$time_iso8601|version=$angie_version|http_metho
   ```

8. В директиве `access_log` укажите способ отправки информации о событиях по протоколу Syslog следующим образом:
   ```
   access_log syslog:server=<IP_коллектора>:<порт> syslog
   ```

9. Если также необходимо отправлять информацию о событиях с ошибками, добавьте строку с директивой `error_log`:
   ```
   error_log syslog:server=<IP_коллектора>:<порт>
   ```

   Формат сообщения из директивы `error_log` невозможно изменить и сообщение всегда передается в следующем виде:

   ```
   YYYY/MM/DD HH:MM:SS [LEVEL] PID#TID: *CID MESSAGE
   ```

   где:

   - `YYYY/MM/DD` – дата в формате год/месяц/день;
   - `HH:MM:SS` – время в формате часы:минуты:секунды;

- `[LEVEL]` – уровень критичности ошибки;
- `PID#TID` – идентификаторы процесса (англ. PID) и потока (англ. TID);
- `*CID` – уникальный номер соединения (англ. Connection ID);
- `MESSAGE` – текст сообщения об ошибке или предупреждении.

10. Проверьте синтаксис в конфигурационном файле на наличие ошибок с помощью команды `sudo angie -t`, как описано в п1 выше.

11. Перезагрузите конфигурацию, выполнив следующую команду:
    ```
    sudo service angie reload
    ```

Передача событий из Angie настроена.

Настройка получения событий Dallas Lock 8

KUMA позволяет осуществлять мониторинг событий системы Dallas Lock 8 версии 11.4.2, поступающих в формате CEF.

Настройка получения событий состоит из следующих этапов:

1. **Настройка отправки событий Dallas Lock 8**
2. **Создание коллектора KUMA для событий Dallas Lock 8**

   При настройке получения событий аудита системы Dallas Lock 8 с помощью мастера установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Confident Dallas Lock syslog CEF**. Также на вкладке **Транспорт** требуется указать порт и протокол в соответствии с пунктами 2.a и 2.b инструкции Настройка отправки событий Dallas Lock 8.
3. **Установка коллектора в сетевой инфраструктуре KUMA**
4. **Проверка поступления событий Dallas Lock 8 в коллектор KUMA**

   Вы можете проверить, что сервер источника событий Dallas Lock 8 настроен правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы**.

Настройка отправки событий Dallas Lock 8

Чтобы настроить отправку событий KUMA:

1. В Dallas Lock 8 перейдите в меню **Выгрузка журналов**.
2. Установите флажок **Экспорт журналов в SIEM-систему** и выполните следующие действия:
   a. В поле **Сервер** укажите IP-адрес или FQDN коллектора KUMA.
   b. В поле **Порт** укажите порт, который прослушивает коллектор KUMA.

c. Выберите формат выгрузки **CEF**.

d. Выберите кодировку выгрузки **UTF-8**.

3. Установите флажки рядом с типами событий, которые необходимо отправлять в KUMA.

4. В раскрывающемся списке **Период выгрузки журналов** выберите значение **1 минута**.

5. Нажмите на кнопку **OK**.

Отправка событий настроена.

Настройка получения событий Единый центр управления Dallas Lock

KUMA позволяет осуществлять мониторинг событий системы Единый центр управления (далее ЕЦУ) Dallas Lock версии 4.0, поступающих в формате CEF.

Настройка получения событий состоит из следующих этапов:

1. **Настройка отправки событий ЕЦУ Dallas Lock**

2. **Создание коллектора KUMA для событий ЕЦУ Dallas Lock**

   При настройке получения событий аудита системы ЕЦУ Dallas Lock с помощью мастера установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Confident Dallas Lock syslog CEF**. Также на вкладке **Транспорт** требуется указать порт и протокол в соответствии с пунктами 2.c, 2.d инструкции Настройка отправки событий Единый центр управления Dallas Lock.

3. **Установка коллектора в сетевой инфраструктуре KUMA**

4. **Проверка поступления событий ЕЦУ Dallas Lock в коллектор KUMA**

   Вы можете проверить, что сервер источника событий ЕЦУ Dallas Lock настроен правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Активные сервисы**.

Настройка отправки событий ЕЦУ Dallas Lock

Чтобы настроить отправку событий ЕЦУ Dallas Lock в KUMA:

1. В ЕЦУ Dallas Lock перейдите в меню **Экспорт инцидентов безопасности**.

2. Установите флажок **Экспорт инцидентов безопасности в SIEM-систему** и выполните следующие действия:

   a. В раскрывающемся списке **Формат** выберите формат **CEF**.

   b. В поле **Сервер** укажите IP-адрес или FQDN коллектора KUMA.

c. В поле **Протокол** укажите протокол, который будет использоваться для передачи данных.

d. В поле **Порт** укажите порт, который прослушивает коллектор KUMA.

3. Нажмите на кнопку **Применить**.

Отправка событий настроена.

Настройка получения событий ProFTPD

KUMA позволяет осуществлять мониторинг событий ProFTPD на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами ProFTPD, после чего события передаются в KUMA через syslog-сервер rsyslog.

Настройка получения событий ProFTPD состоит из следующих этапов:

1. Настройка аудита событий ProFTPD
2. Создание коллектора KUMA для событий ProFTPD

   При создании коллектора в веб-интерфейсе KUMA на шаге **Транспорт** нужно указать порт и протокол, которые используются при настройке syslog-сервера для отправки событий. Для получения событий аудита из ProFTPD на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Proftpd syslog**.
3. Установка коллектора в сетевой инфраструктуре KUMA
4. Настройка syslog-сервера для отправки событий
5. **Проверка поступления событий ProFTPD в коллектор KUMA**

   Вы можете проверить, что настройка поступления событий из ProFTPD выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка аудита событий ProFTPD

Чтобы настроить аудит событий в системе ProFTPD:

1. Создайте резервную копию конфигурационного файла /etc/proftpd/proftpd.conf.

2. Откройте файл proftpd.conf и добавьте или измените значения следующих параметров:

```
LogFormat default "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
LogFormat auth "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
ExtendedLog /var/log/proftpd/access.log ALL default
ExtendedLog /var/log/proftpd/auth.log AUTH auth
```

3. Сохраните изменения и перезапустите сервис, выполнив команду:

```
sudo systemctl restart proftpd
```

Аудит событий ProFTPD будет настроен.

Система ProFTPD не выполняет ротацию журналов. Чтобы снизить риск переполнения дискового пространства, рекомендуется использовать внешние инструменты ротации журналов, например Logrotate или Logadm.

Настройка syslog-сервера для отправки событий ProFTPD

Для передачи событий от сервера в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена система ProFTPD, в коллектор:

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В директории /etc/rsyslog.d создайте файл proftpd.conf со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<IP-адрес коллектора KUMA>" port="<порт коллектора KUMA>" protocol="tcp")
     stop
     }
     ```

   - Для отправки событий по протоколу UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<IP-адрес коллектора KUMA>" port="<порт коллектора KUMA>" protocol="udp")
     stop
     }
     ```

3. Сохраните изменения в файле proftpd.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях будут передаваться с сервера в коллектор KUMA.

Настройка получения событий Vsftpd

KUMA позволяет осуществлять мониторинг событий Vsftpd на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами Vsftpd, после чего события передаются в KUMA через syslog-сервер rsyslog.

Настройка получения событий Vsftpd состоит из следующих этапов:

1. **Настройка аудита событий Vsftpd**
2. **Создание коллектора KUMA для событий Vsftpd**

   При создании коллектора в веб-интерфейсе KUMA на шаге **Транспорт** нужно указать порт и протокол, которые используются при настройке syslog-сервера для отправки событий. Для получения событий аудита из Vsftpd на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Vsftpd syslog**.
3. **Установка коллектора в сетевой инфраструктуре KUMA**
4. **Настройка syslog-сервера для отправки событий**
5. **Проверка поступления событий Vsftpd в коллектор KUMA**

   Вы можете проверить, что настройка поступления событий из Vsftpd выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка аудита событий Vsftpd

Чтобы настроить аудит событий в системе Vsftpd:

1. Создайте резервную копию конфигурационного файла /etc/vsftpd/vsftpd.conf.
2. Откройте файл vsftpd.conf и добавьте или измените значения следующих параметров:

```
xferlog_enable=YES
xferlog_std_format=NO
xferlog_file=/var/log/vsftpd.log
log_ftp_protocol=YES
```

3. Сохраните изменения и перезапустите сервис, выполнив команду:

```
sudo systemctl restart vsftpd
```

Аудит событий Vsftpd будет настроен.

Система Vsftpd не выполняет ротацию журналов. Чтобы снизить риск переполнения дискового пространства, рекомендуется использовать внешние инструменты ротации журналов, например Logrotate или Logadm.

Настройка syslog-сервера для отправки событий Vsftpd

Для передачи событий от сервера в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена система Vsftpd, в коллектор:

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В директории /etc/rsyslog.d создайте файл vsftpd.conf со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @@<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
     ```

     Например:

     ```
     *.* @@192.1.3.4:5858
     ```

   - Для отправки событий по протоколу UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
     ```

     Например:

     ```
     *.* @192.1.3.4:5858
     ```

3. Сохраните изменения в файле vsftpd.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях будут передаваться с сервера в коллектор KUMA.

Настройка получения событий HAProxy

KUMA позволяет осуществлять мониторинг событий балансировщика нагрузки HAProxy (версия 2.4) в форматах HTTP, TCP, HTTP CLF, Default, HTTPS (для версии 2.6 и выше), TCP CLF (для версии 3.2 и выше), поступающих по протоколу syslog.

Настройка получения событий HAProxy состоит из следующих этапов:

1. Настройка передачи событий HAProxy
2. Создание коллектора KUMA для событий HAProxy

   Для получения событий HAProxy в мастере установки коллектора на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] HAProxy syslog**, а на шаге **Транспорт** нужно выбрать тип коннектора **udp**.
3. Установка коллектора в сетевой инфраструктуре KUMA
4. **Проверка поступления событий HAProxy в коллектор KUMA**

   Вы можете проверить, что поступление событий из HAProxy настроено правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка передачи событий HAProxy

Чтобы настроить передачу событий HAProxy:

1. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду:

   ```
   haproxy -c -V -f /etc/haproxy/haproxy.cfg
   ```

   Возможные сообщения при проверке конфигурационного файла

   Если в конфигурационном файле синтаксические ошибки отсутствуют, HAProxy отобразит уведомление `Configuration file is valid`.

   Если в конфигурационном файле найдены синтаксические ошибки, HAProxy сообщит, в чем заключается ошибка, например:

   `[NOTICE] (284146): haproxy version is 2.4.24-0ubuntu0.22.04.2`

   `[NOTICE] (284146): path to executable is /usr/sbin/haproxy`

   `[ALERT] (284146): parsing [/etc/haproxy/haproxy.cfg:25] : unknown option 'httpdlog'; did you mean 'httplog' maybe ?`

   `[ALERT] (284146): Error(s) found in configuration file : /etc/haproxy/haproxy.cfg`

   `[ALERT] (284146): Fatal errors found in configuration`

Подробнее о синтаксисе конфигурационного файла см. в официальной документации HAProxy.

2. Если проверка синтаксиса прошла успешно, выполните резервное копирование исходного конфигурационного файла с помощью следующей команды:

   ```
   sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy_backup.cfg
   ```

3. Откройте конфигурационный файл haproxy.cfg, выполнив следующую команду:

   ```
   sudo vi /etc/haproxy/haproxy.cfg
   ```

   Дальнейшие шаги инструкции предполагают, что для всех групп серверов применяются единые параметры записи в журнал. В этом случае параметры записи в журнал указываются в секции `global`, а в секции `defaults` используется строка `log global`.

   Если требуется более детальная настройка записи в журнал, нужно удалить строку `log global` из секции `defaults`. Так как секции `frontend`, `backend` и `listen` по умолчанию наследуют параметры из секции `defaults`, это приведет к отключению глобальной записи в журнал. В таком случае необходимо определить параметры записи в журнал в каждой секции, добавив строку следующего вида:

   ```
   log <IP_адрес_коллектора_KUMA> [len <длина_в_байтах>] [format
   <формат_syslog_сообщения>] [sample <диапазоны>:<размер_выборки>] <facility>
   [<уровень> [<минимальный_уровень>]]
   ```

4. В секции `global` укажите IP-адрес коллектора KUMA:

   ```
   log <IP-адрес_коллектора>:<порт>
   ```

5. В секции `global` добавьте следующую строку для добавления имени хоста в заголовок syslog:

   ```
   log-send-hostname <имя_хоста>
   ```

6. В секции `defaults` добавьте строку для использования глобальных параметров записи в журнал:

   ```
   log global
   ```

7. В секции `defaults` укажите формат журналирования:

   - Для балансировщиков 4 уровня (TCP):

     ```
     option tcplog
     ```

     Пример секции defaults с настроенными параметрами

     ```
     defaults
     log global
     mode tcp
     option tcplog
     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
     ```

   - Для балансировщиков 7 уровня (HTTP):

     ```
     option httplog
     ```

Пример секции defaults с настроенными параметрами

```
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
```

8. Если требуется включить запись в журнал HTTP-заголовков запроса, добавьте в секцию `frontend` или `listen` строку:

   `capture request header <имя_заголовка> len <длина_заголовка_в_байтах>`

   Каждый заголовок необходимо указывать отдельной строкой, например:

   `capture request header User-agent len 50`

   `capture request header Host len 30`

   `capture request header X-Forwarded-For len 15`

9. Если требуется включить запись в журнал HTTP-заголовков ответа, добавьте в секцию `frontend` или `listen` строку:

   `capture response header <имя_заголовка> len <длина_заголовка_в_байтах>`

   Каждый заголовок необходимо указывать отдельной строкой, например:

   `capture response header User-agent len 50`

   `capture response header Host len 30`

   `capture response header X-Forwarded-For len 15`

10. Если требуется включить запись в журнал HTTP-cookie, добавьте в секцию `frontend` или `listen` строку:

    `capture cookie <имя_cookie> len <размер_cookie_в_байтах>`

    В журнал записывается только первый файл cookie с указанным именем.

11. Проверьте синтаксис в конфигурационном файле на наличие ошибок с помощью команды `haproxy -c -V -f /etc/haproxy/haproxy.cfg`, как описано в пункте 1.

12. Перезагрузите конфигурацию, выполнив следующую команду:

    `sudo systemctl reload haproxy`

13. Проверьте, что балансировщик нагрузки HAProxy запущен и работает правильно, выполнив следующую команду:

    `sudo systemctl status haproxy`

Передача событий из HAProxy будет настроена.

Настройка получения событий Veeam Backup & Replication

KUMA позволяет осуществлять мониторинг событий системы Veeam Backup & Replication (версия 12.1), поступающих по протоколу syslog.

Настройка получения событий Veeam Backup & Replication состоит из следующих этапов:

1. Настройка передачи событий Veeam Backup & Replication
2. Создание коллектора KUMA для событий Veeam Backup & Replication

   При создании коллектора в веб-интерфейсе KUMA на шаге **Транспорт** нужно указать тип коннектора, который используется при настройке передачи событий. Для получения событий Veeam Backup & Replication на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Veeam Software Veeam Backup & Replication syslog**.
3. Установка коллектора в сетевой инфраструктуре KUMA
4. **Проверка поступления событий Veeam Backup & Replication в коллектор KUMA**

   Вы можете проверить, что поступление событий из Veeam Backup & Replication настроено правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка передачи событий Veeam Backup & Replication

Настройку передачи событий необходимо выполнять под учетной записью с правами администратора.

Чтобы настроить передачу событий Veeam Backup & Replication по syslog:

1. В веб-интерфейсе Veeam Backup & Replication откройте раздел **Параметры** → **Пересылка событий**.
2. В разделе **Серверы Syslog** нажмите **Добавить**.
3. В поле **Сервер** укажите полное доменное имя (FQDN) или IPv4-адрес сервера коллектора KUMA. Указать IPv6-адрес в этом поле невозможно.
4. В поле **Порт** укажите порт, который прослушивает коллектор KUMA.

   По умолчанию система Veeam Backup & Replication выполняет отправку событий на следующие порты в зависимости от используемого протокола:

   - 514 для TCP и UDP;
   - 6514 для TLS.
5. В раскрывающемся списке **Транспорт** выберите протокол: **TCP**, **UDP** или **TLS**.
6. Нажмите **OK**.

Передача событий из Veeam Backup & Replication в коллектор KUMA будет настроена.

Настройка получения событий Apache Tomcat

KUMA позволяет осуществлять мониторинг событий аудита веб-сервера Apache Tomcat версий 9.0 и выше, 10.1 и выше и 11.0 и выше, развернутого на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами Apache Tomcat, после чего события передаются в KUMA через syslog-сервер rsyslog.

Настройка получения событий Apache Tomcat состоит из следующих этапов:

1. Настройка аудита событий Apache Tomcat
2. Создание коллектора KUMA для событий Apache Tomcat

   Для получения событий Apache Tomcat в мастере установки коллектора KUMA на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Apache Tomcat**.
3. Установка коллектора в сетевой инфраструктуре KUMA
4. Настройка syslog-сервера для отправки событий
5. **Проверка поступления событий Apache Tomcat в коллектор KUMA**

   Вы можете проверить, что настройка поступления событий из Apache Tomcat выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Настройка аудита событий Apache Tomcat

Чтобы настроить аудит событий в системе Apache Tomcat:

1. Подключитесь по протоколу SSH к серверу Apache Tomcat под учетной записью с правами администратора.

   > Дальнейшие шаги инструкции предполагают, что на сервере настроены стандартные переменные среды `$CATALINA_HOME` и `$JAVA_HOME`.

   Подробнее о переменных см. в руководстве по установке Apache Tomcat.

2. Выполните резервное копирование исходного конфигурационного файла с помощью команды:

   ```
   sudo cp $CATALINA_HOME/conf/server.xml $CATALINA_HOME/conf/server_backup.xml
   ```

3. Откройте конфигурационный файл Apache Tomcat с помощью команды:

   ```
   sudo vi $CATALINA_HOME/conf/server.xml
   ```

4. Найдите элемент `<Valve className="org.apache.catalina.valves.AccessLogValve" ... />` и замените его на следующий вариант с использованием `JsonAccessLogValve`:

   ```
   <Valve className="org.apache.catalina.valves.JsonAccessLogValve" directory="logs"
     prefix="access_log" suffix=".txt"
     maxDays="7"
     pattern="%h %a %t %m %U %q %r %H %A %v %p %s %b %X %I %{User-Agent}i %{Cookie}c"/>
   ```

Если невозможно использовать `JsonAccessLogValve`, оставьте `AccessLogValve`, но задайте расширенный шаблон, чтобы увеличить объем собираемых полей:

```
pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocol=
Agent=%{User-Agent}i|Cookie=%{Cookie}c"
```

Пример конфигурации с `AccessLogValve`:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
  prefix="access_log" suffix=".txt"
  maxDays="7"
  pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocc
  Agent=%{User-Agent}i|Cookie=%{Cookie}c"/>
```

Нормализатор также поддерживает шаблоны Common и Combined для `AccessLogValve` и `JsonAccessLogValve`.

5. Перезапустите веб-сервер Apache Tomcat с помощью следующих команд:

```
sudo $CATALINA_HOME/bin/shutdown.sh
sudo $CATALINA_HOME/bin/startup.sh
sudo systemctl restart tomcat.service
```

Аудит событий Apache Tomcat будет настроен.

Настройка syslog-сервера для отправки событий Apache Tomcat

Для передачи событий от сервера в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена система Apache Tomcat, в коллектор:

1. Проверьте, что на сервере, являющимся источником событий, установлен сервис rsyslog. Для этого выполните следующую команду:

```
systemctl status rsyslog.service
```

Если сервис запущен, то отобразится уведомление следующего вида:

```
Active: active (running) since Tue 2025-09-23 15:31:30 MSK; 1 week 0 days ago
```

Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

```
sudo apt install rsyslog
sudo systemctl enable rsyslog.service
sudo systemctl start rsyslog.service
```

2. Проверьте синтаксис в конфигурационном файле с помощью следующей команды:

```
rsyslogd -N1
```

Возможные сообщения при проверке конфигурационного файла

Если в конфигурационном файле синтаксические ошибки отсутствуют, сервис rsyslog отобразит следующие уведомления:

```
rsyslogd: version 8.2112.0, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

Если в конфигурационном файле найдены синтаксические ошибки, сервис rsyslog сообщит, в чем заключается ошибка, например:

```
rsyslogd: version 8.2112.0, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
https://www.rsyslog.com/e/2221 ]
rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
https://www.rsyslog.com/e/2221 ]
rsyslogd: parameter "maxLinesAtOnce" not permited in inotify mode - ignored [v8.2112.0
try https://www.rsyslog.com/e/2222 ]
rsyslogd: $WorkDirectory: /var/lib/rsyslog not a directory - directive ignored
[v8.2112.0 try https://www.rsyslog.com/e/2181 ]
rsyslogd: imfile: no working or state file directory set, imfile will create state
files in the current working directory (probably the root dir). Use
global(workDirectory="/some/path") to set the working directory [v8.2112.0 try
https://www.rsyslog.com/e/2450]
```

3. Откройте конфигурационный файл rsyslog.conf, выполнив следующую команду:

```
sudo vi /etc/rsyslog.conf
```

4. Проверьте, что в файле указана строка, разрешающая загрузку конфигураций из директории /etc/rsyslog.d, выполнив следующие команды

```
# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")
```

5. Создайте конфигурационный файл apache_tomcat_to_siem.conf в директории /etc/rsyslog.d/ с помощью следующей команды:

```
sudo touch /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

6. Откройте созданный конфигурационный файл apache_tomcat_to_siem.conf с помощью следующей команды:

```
sudo vi /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

7. Выполните следующую команду, чтобы узнать абсолютный путь к директории Apache Tomcat:

```
printenv CATALINA_HOME
```

> Абсолютный путь нужен для того, чтобы указать его в конфигурационном файле, так как сервис rsyslog не поддерживает использование переменных окружения.

8. Добавьте в конфигурационный файл правила для чтения `Access Log` и пересылки данных на коллектор KUMA:

```
input(
        type="imfile"
        File="<абсолютный_путь_из_пункта 7>/logs/access_log*.txt"
        Tag="apachetomcat"
)
if $programname == "apachetomcat" then {
        action(
                type="omfwd"
                target="<FQDN_или_IP-адрес_коллектора_KUMA"
                port="<порт_коллектора_KUMA"
                protocol="udp_или_tcp"
        )
}
```

9. Проверьте синтаксис в конфигурационном файле на наличие ошибок с помощью команды `sudo rsyslogd -N1`, как описано в пункте 2.

10. Перезагрузите сервис rsyslog с помощью команды:

    ```
    sudo systemctl restart rsyslog
    ```

11. Проверьте, что сервис rsyslog запущен и работает правильно, выполнив следующую команду:

    ```
    sudo systemctl status rsyslog
    ```

Передача событий от сервера, на котором установлена система Apache Tomcat, в коллектор будет настроена.

Мониторинг источников событий

В этом разделе представлена информация о мониторинге источников событий.

https://rutube.ru/video/4dae62d146a819a2044fbc45f07ac65a/

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, используя один из следующих наборов полей:

- Пользовательский набор полей. Вы можете указать от 1 до 9 полей в желаемой последовательности. TenantID отдельно задавать не нужно, определяется автоматически.

- **Применить сопоставление по умолчанию**: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Порядок полей не подлежит изменению.

Определение источников происходит, если следующие поля в событиях содержат непустые значения: DeviceProduct + DeviceAddress и/или DeviceHostname + TenantID (отдельно задавать это поле не нужно, определяется автоматически). Поле DeviceProcessName может содержать пустое значение. Если поле DeviceProcessName содержит непустое значение, и остальные обязательные поля заполнены, будет определен новый источник.

Определение источников событий в зависимости от наличия непустых значений в полях событий

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (определяется автоматически)	
+	+			+	Определятся источник 1
+		+		+	Определятся источник 2
+	+	+		+	Определятся источник 3
+	+		+	+	Определятся источник 4
+		+	+	+	Определятся источник 5
+	+	+	+	+	Определятся источник 6
	+	+		+	Источник не определяется
	+		+	+	Источник не определяется
		+	+	+	Источник не определяется
+			+	+	Источник не определяется

Применяется только один набор полей для всей инсталляции. При обновлении на новую версию KUMA применяется набор полей по умолчанию. Настраивать набор полей для определения источника событий может только пользователь с ролью Главный администратор. После того как вы сохраните изменения в наборе полей, ранее определенные источники событий будут удалены из веб-интерфейса 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 KUMA начала определять источники с учетом новых параметров, перезапустите коллекторы.

Чтобы определить источники событий:

1. В веб-интерфейсе KUMA перейдите в раздел **Состояние источников**.

2. На вкладке **Список источников событий** в меню ⋮ нажмите **Настройки**.

3. В открывшемся окне **Настройки определения источников** в раскрывающемся списке **Группирующие поля для определения источника** выберите поля событий, по которым вы хотите определять источники событий.

   Вы можете указать от 1 до 9 полей в желаемой последовательности. В пользовательской конфигурации KUMA определяет источники, в которых заполнено поле TenantID (отдельно задавать это поле не нужно, определяется автоматически) и хотя бы одно поле из указанных в списке **Группирующие поля для определения источника**. Для числовых полей 0 является пустым значением. Если для определения источников выбрано одно числовое поле и значение числового поля равно 0, источник не будет определен.

   После того, как вы сохраните измененный набор полей, будет создано событие аудита и все ранее определенные источники будут удалены из веб-интерфейса KUMA и из базы данных, назначенные политики будут отключены.

4. Если вы хотите вернуться к списку полей для определения источника событий по умолчанию, нажмите **Применить сопоставление по умолчанию**. Порядок полей по умолчанию не подлежит изменению. Если вы вручную укажете поля в неверном порядке, появится ошибка и кнопка сохранения настроек будет недоступна. Корректная последовательность полей по умолчанию: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Минимальная конфигурация для определения источников событий с использованием набора событий по умолчанию: непустые значения в полях событий DeviceProduct + DeviceAddress и\или DeviceHostName + TenantID (определяется автоматически).

5. Нажмите **Сохранить**.

6. Перезапустите коллекторы, чтобы изменения вступили в силу и источники событий начали определяться по заданному списку полей.

Настройка определения источников выполнена.

Чтобы просмотреть события, которые относятся к источнику событий:

1. В веб-интерфейсе KUMA перейдите в раздел **Состояние источников**.

2. В открывшемся окне **Список источников событий** выберите в списке нужный источник событий и в столбце **Название** разверните меню для выбранного источника событий, нажмите на кнопку **событий за <количество> дней**.

   KUMA выполнит переход в раздел **События**, где вы сможете просмотреть список событий для выбранного источника за последние 5 минут. В запросе автоматически будут указаны значения полей, заданных в параметрах определения источника событий. При необходимости в разделе **События** можно изменить в запросе временной интервал и нажать **Выполнить запрос** повторно, чтобы просмотреть выборку за указанный промежуток времени.

Ограничения

1. В конфигурации с использованием набора полей по умолчанию KUMA регистрирует источник событий при условии, что поля DeviceProduct + DeviceAddress и\или DeviceHostName содержатся в сыром событии.

   Если сырое событие не содержит поля DeviceProduct + DeviceAddress и\или DeviceHostName, вы можете выполнить следующие действия:

   - Настроить обогащение в нормализаторе: на вкладке нормализатора **Обогащение** выберите тип данных **Событие**, укажите значения для параметра **Исходное поле**, для параметра **Целевое поле** выберите DeviceProduct + DeviceAddress и\или DeviceHostName и нажмите 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 полей, определяющих 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 решения 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 веб-интерфейсе KUMA в разделе **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 **Состояние источников** → **Список источников событий**. Таблицу можно сортировать, нажав на заголовок столбца нужного параметра и выбрав **По возрастанию** или **По убыванию**.

Источники событий можно искать по названию с помощью поля **Поиск**. Для поиска по одному символу введите этот символ и нажмите на клавишу `Enter`. 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

В разделе **Состояние источников** → **Список источников событий** доступны следующие столбцы с информацией об источниках событий:

- **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 назначенной политики мониторинга;

  - серый – источнику событий не присвоены 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. Название 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 в кодировке Unicode.

- **Имя хоста или IP-адрес** – название хоста или IP-адрес, откуда поступают события, если в параметрах определения источников событий заданы 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**. Для поиска политики по одному символу введите этот символ и нажмите на клавишу `Enter`.

  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 по каждой политике. 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, в поле **Поток** отображаются источники с количеством событий. Если источнику назначены политики мониторинга только типа **byEPS** или политики не назначены, в поле **Поток** отображаются источники с количеством событий в секунду.

  При сортировке по столбцу **Поток** сначала отображаются источники с количеством событий в секунду (**byEPS**), а затем – с количеством событий (**byCount**).

  После получения запроса пользователя KUMA отбирает нужные источники событий и сортирует их их по значениям столбца **Поток** на момент получения запроса. После чего значения в этом столбце обновляются в соответствии с запросом пользователя.

Отображаемое значение может не соответствовать сортировке из-за динамического обновления данных о событиях в источниках для предоставления актуальной информации.

- **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 отключению 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:

- **Включить политику** – с помощью этой кнопки для источников событий можно включить политику мониторинга. При применении требуется выбрать политики в открывшемся окне.

- **Отключить политику** – с помощью этой кнопки для источников событий можно отключить политику мониторинга. При отключении 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 на источники 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 прежняя 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 на источник события была назначена политика мониторинга, тогда в выгружаемом файле будет указана единица измерения потока, взятая из политики. Если политика не назначена, пустое поле `Stream` - это ожидаемое поведение.

- **Построить диаграмму** – 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 файле CSV

Вы можете скачать информацию об одном или нескольких источниках событий и примененных к ним политикам мониторинга в файл CSV в кодировке UTF-8 и с запятой в качестве разделителя. Если к источнику применены несколько политик мониторинга, в файле для этого источника каждая политика мониторинга и ее параметры записываются на отдельной строке. Для каждой политики мониторинга, примененной к источнику файл содержит следующие параметры: **Статус**, **Название**, **Политика мониторинга**, **Нижний порог**, **Верхний порог**, **Поток**, **Тенант**. Группирующие поля для определения источников сохраняются в файле CSV в порядке, установленном пользователем при настройке определения источников. При скачивании данных по нескольким источникам выбранный в веб-интерфейсе KUMA порядок источников не сохраняется. Если вы хотите отсортировать список источников, вы можете сделать это в Excel или выполнить grep с сортировкой.

Чтобы скачать информацию об источниках событий в файл CSV:

1. В веб-консоли KUMA в разделе **Состояние источников** → **Список источников 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 несколько источников событий в таблице, установив флажок в заголовке первого столбца 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. При этом снять флажок с отдельного источника событий невозможно.

   - **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. После выбора всех источников на странице можно снять флажок с отдельных источников событий.

2. Нажмите на кнопку **CSV** в верхней части таблицы.

   > В зависимости от размера окна вашего браузера кнопка **CSV** может находиться в меню ⋮.

   Задача экспорта источников событий будет создана в диспетчере задач.

3. Перейдите в раздел **Диспетчер задач** и найдите созданную задачу.

   Когда файл будет готов, в строке задачи в столбце **Статус** отобразится статус **Завершено**.

4. Нажмите на название типа задачи и в раскрывающемся списке выберите **Скачать**.

CSV-файл с информацией об источниках будет скачан с использованием параметров вашего браузера. Имя файла по умолчанию event-source-list_YYYYMMDD_HHMMSS.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).

Просмотреть график для одного источника событий вы можете в веб-консоли KUMA в разделе **Состояние источников** → **Список источников событий**, нажав на значок стрелки › в строке нужного 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 в 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 веб-консоли KUMA в разделе **Состояние источников** → **Список источников событий** выберите в таблице один или несколько источников событий, установив флажки в первом столбце напротив нужных источников.

   Вы можете построить диаграмму максимум для 5 источников событий одновременно.

2. Нажмите на кнопку **Построить диаграмму** в верхней части таблицы.

   > В зависимости от размера окна вашего браузера кнопка **Построить диаграмму** 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.

Политики мониторинга можно искать с помощью поля **Поиск**. Поиск будет осуществляться по столбцам **Название**, **Тенант**, **Тип**, **Расписание** (название дня и время). Для поиска политики по одному символу введите этот символ и нажмите на клавишу `Enter`.

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 **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 в раздел **Список источников 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 Victoria Metrics, и глубина хранения данных на сервере Ядра KUMA составляет 15 суток.

4. Один раз в минуту выполняется инвентаризация источников событий.

5. Поток подсчитывается отдельно для каждого источника событий по следующим правилам:

   - Если к источнику событий применяется политика мониторинга, то отображаемое отображается 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 в количестве событий (для типа политики **byCount** или для политик разных типов) или в количестве событий в секунду (EPS, для политики типа **byEPS**). Вы можете узнать, в чем считается поток для назначенной политики, в столбце **Поток** на странице **Список источников 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. Один раз в минуту поток событий проверяется на соответствие параметрам политики.

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`). Событие имеет поля, описанные в таблице ниже.

Поля события мониторинга

Название поля события	Значение поля
ID	Уникальный идентификатор события.
Timestamp	Время события.
Type	Тип события аудита. Событию аудита соответствует значение `5` (мониторинг).
Name	Имя политики мониторинга.
DeviceProduct	`KUMA`
DeviceCustomString1	Значение из поля `value` в уведомлении. Отображает 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 веб-интерфейсе KUMA в разделе **Состояние источников** → **Политики мониторинга** нажмите **Добавить политику** и в открывшемся окне укажите параметры политики мониторинга.

2. В поле **Название политики** введите имя создаваемой политики. Название должно содержать от 1 до 128 символов в кодировке Unicode и быть уникальным в рамках выбранного тенанта.

   Мы рекомендуем 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 поле **Нижний порог** и **Верхний порог** определите, выход за какие границы будет считаться отклонением от нормы, при котором политика мониторинга будет срабатывать, создавая алерт и рассылая 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 выбран интервал 5 минут.

   При указании интервала оценки учитывайте расписание применения политики. Например, если вы указали применение политики ежедневно раз в несколько часов, мы не рекомендуем 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**. Вы можете 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 отправляемых 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 регулярность 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 промежутка 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 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 промежутка 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 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 **Добавить**.

Политика мониторинга добавлена.

Изменение политики мониторинга

В разделе **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 если да, 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**.
  - **Расписание**.

    Изменения в расписании применяются в течение минуты, когда KUMA проверяет наличие политик, которые должны включиться или выключиться.

- **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**.

    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 веб-консоли KUMA в разделе **Состояние источников** → **Список источников событий** выберите в таблице один или несколько источников событий, установив флажки в первом столбце напротив нужных источников. Вы можете выбрать сразу несколько источников событий в списке, нажав на флажок в первом столбце в заголовке таблицы и выбрав одно из следующих значений:
   - **Выбрать все** – выберите все источники событий на всех страницах таблицы. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники, удовлетворяющие условию поиска. При этом снять флажок с отдельного источника событий невозможно.
   - **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. После выбора всех источников на странице можно снять флажок с отдельных источников событий.

   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, на панели инструментов станет доступна кнопка **Включить политику**.
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 будут 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. Мы рекомендуем 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 веб-консоли KUMA в разделе **Состояние источников** → **Список источников 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. 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, нажав на флажок в первом столбце в заголовке таблицы и выбрав одно из следующих значений:

- **Выбрать все** – выберите 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, от 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 от них нужные политики.
- Отфильтровать таблицу источников по какому-либо параметру таким образом, чтобы в таблице отобразилось до 100 000 источников включительно, и отключить от 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 новую политику мониторинга на основе существующей:

1. В веб-интерфейсе KUMA в разделе **Состояние источников** → **Политики мониторинга** выберите политику мониторинга, на основе которой вы хотите создать новую политику.

   При необходимости вы можете найти необходимые политики мониторинга с помощью поля **Поиск**. Поиск будет осуществляться по столбцам **Название**, **Тенант**, **Тип**, **Расписание** (название дня и время). Для поиска политики по одному символу введите этот символ и нажмите на клавишу `Enter`.

2. Нажмите **Дублировать политику**.

3. В открывшемся окне **Добавить политику** измените параметры политики.

   По умолчанию в название новой политики будет добавлено `- копия`. Остальные параметры будут такие же, как в дублируемой политике.

4. Нажмите на кнопку **Добавить**, чтобы создать новую политику.

Политика мониторинга будет создана на основе существующей политики.

Удаление политики мониторинга

Чтобы удалить политику мониторинга:

1. В веб-интерфейсе KUMA в разделе **Состояние источников** → **Политики мониторинга** 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** (название дня и время). Для поиска политики по одному символу введите этот символ и нажмите на клавишу **`Enter`**.

2. Нажмите **Удалить политику** и подтвердите действие.

Выбранные политики мониторинга будут удалены.

> Невозможно удалить предустановленные политики мониторинга, а также политики, назначенные источникам событий.

Управление активами

Активы представляют собой устройства и системы в организации, для которых поступают события безопасности. Это могут быть рабочие станции, серверы, сетевое оборудование, мобильные устройства и другие объекты инфраструктуры. После добавления активов в KUMA их идентификаторы будут добавляться при обогащении событий и при анализе событий вы получите дополнительную информацию о компьютерах в организации.

Вы можете просматривать информацию об активах, искать активы по заданным критериям, редактировать их и удалять, а также экспортировать данные о них в CSV-файл.

Категории активов

Вы можете сгруппировать активы по категориям, которые можно использовать при настройке 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 KUMA категориям активов присвоены следующие уровни важности: Низкий, Средний, Высокий, Критичный. 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. Если вы указали относительный период и выбрали регулярность категоризации, например, каждый час, при каждом запуске категоризации условие будет учитывать информацию об активах, актуальную на момент запуска категоризации.

  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 с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

     Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	=, ilike	
ОС	=, ilike	Оператор **ilike** 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.
Полное доменное имя	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Уровень критичности уязвимостей CVE на активе. Возможные значения параметра CVSS – от 0 до 10. Для уязвимостей из Kaspersky Security Center неприменимо.

Количество CVE	>, >=, =, <=, <	Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Для категоризации по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		`И`
		`CVSS >= 6.5`

ПО	=, ilike	Категоризация по ПО, установленному на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
Версия ПО	=, ilike, in	Категоризация по номеру версии (сборки) ПО, установленного на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
КИИ	in	Можно выбрать более одного значения.
Группа KSC	=, ilike	Категоризация по названию группы администрирования Kaspersky Security Center, в которую помещен актив.

Последнее обновление антивирусных баз	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление информации	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление защиты	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Время начала последней сессии	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Статус 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	=	

Последнее появление в сети	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Рейтинг AI	>,>=,=,<=,<	Категоризация по рейтингам активов, присвоенным AI-сервисами.
Статус	=, in	Категоризация по предустановленным статусам актива, присвоенным AI-сервисами.
Настраиваемое поле актива	=, ilike	Категоризация по значениям настраиваемых полей 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 запуска категоризации 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 регулярно привязывать к категории активы, для которых антивирусные базы не обновлялись более 1 часа до запуска категоризации.

   - 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 регулярно привязывать к категории активы, информация о которых обновилась за сутки до запуска категоризации; или указать значение **now/w** с оператором **<=**, чтобы регулярно привязывать к категории 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**.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно**: при срабатывания корреляционного правила актив будет перемещаться в указанную группу.

В KUMA 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** веб-интерфейса KUMA. 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 автоматическое обновление активов в выбранной категории. В процессе обновления могут быть привязаны новые активы или исключены ранее привязанные. 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 опция **Удалить категорию** будет неактивна.
Сделать закладкой	Отобразить выбранную категорию на отдельной вкладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из закладок**.

Добавление категории активов

Чтобы добавить категорию активов:

1. Откройте раздел **Активы** веб-интерфейса KUMA.

2. Откройте окно создания категории, выполнив следующие действия:

   a. В списке тенантов раскройте тенант, в который вы хотите добавить новую категорию.

   b. Наведите курсор мыши на родительскую категорию и выполните одно из следующих действий:

      - Нажмите на значок плюса (+).

      - В меню (⋮) выберите **Добавить подкатегорию**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить категорию**.

3. Добавьте сведения о категории:

   - В поле **Название** введите название категории. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   - При необходимости в раскрывающемся списке **Родительская категория** измените категорию.

   - В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию. Изменить выбранный ранее тенант невозможно.

   - При необходимости в раскрывающемся списке **Уровень важности** измените уровень важности категории. Значение по умолчанию: **Низкий**.

   - При необходимости в поле **Описание** добавьте примечание: до 4000 символов в кодировке Unicode.

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 условию. Если активы больше не удовлетворяют этому условию, такие активы будут отвязываться от категории независимо от того, были ли активы добавлены автоматически или вручную.

     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 с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	=, ilike	
ОС	=, ilike	Оператор **ilike** 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.
Полное доменное имя	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Уровень критичности уязвимостей CVE на активе. Возможные значения параметра CVSS – от 0 до 10. Для уязвимостей из Kaspersky Security Center неприменимо.

Количество CVE	>, >=, =, <=, <	Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Для категоризации по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		И
		`CVSS >= 6.5`

ПО	=, ilike	Категоризация по ПО, установленному на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
Версия ПО	=, ilike, in	Категоризация по номеру версии (сборки) ПО, установленного на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
КИИ	in	Можно выбрать более одного значения.
Группа KSC	=, ilike	Категоризация по названию группы администрирования Kaspersky Security Center, в которую помещен актив.
Последнее обновление антивирусных баз	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.

Последнее обновление информации	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление защиты	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Время начала последней сессии	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Статус 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	=	

Последнее появление в сети	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Рейтинг AI	>,>=,=,<=,<	Категоризация по рейтингам активов, присвоенным AI-сервисами.
Статус	=, in	Категоризация по предустановленным статусам актива, присвоенным AI-сервисами.
Настраиваемое поле актива	=, ilike	Категоризация по значениям настраиваемых полей 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 запуска категоризации 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 регулярно привязывать к категории активы, для которых антивирусные базы не обновлялись более 1 часа до запуска категоризации.

   - 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 регулярно привязывать к категории активы, информация о которых обновилась за сутки до запуска категоризации; или указать значение **now/w** с оператором **<=**, чтобы регулярно привязывать к категории 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**.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите **Сохранить**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В KUMA можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы активов:

1. Откройте раздел **Активы** веб-интерфейса KUMA.

2. В правом верхнем углу таблицы активов нажмите значок шестеренки (⚙).

3. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:

   - **Полное доменное имя**

   - **IP-адрес**

   - **Источник актива**

   - **Владелец**

- **MAC-адрес**
- **Создан**
- **Последнее обновление**
- **Тенант**
- **Категория КИИ**
- **Архивный**
- **Статус**
- **Рейтинг AI**

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 KUMA 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:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на кнопку .

   В верхней части окна отображается поле **Поиск**.

2. Введите поисковый запрос в поле **Поиск** и нажмите **ENTER** или значок .

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 **Активы** веб-интерфейса KUMA нажмите на кнопку .

   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 Kaspersky Security Center неприменимо.

Левый операнд	Доступные операторы	Правый операнд

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	• Kaspersky Security Center. • 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 Kaspersky Security Center, 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*.

Левый операнд	Доступные операторы	Правый операнд
Время начала последней сессии	>=, <=	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	• Хост с установленным Агентом администрирования подключен 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 хосте установлено одно или несколько несовместимых приложений. • Хост имеет одну или несколько уязвимостей. • Последний поиск обновлений операционной системы на хосте выполнялся слишком давно. • Хост не имеет надлежащего статуса шифрования. • Параметры мобильного устройства не соответствуют требованиям политики безопасности. • Есть необработанные инциденты. • Статус хоста был предложен управляемым продуктом. • На хосте 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 хосте нет правил шифрования. • Шифрование выполняется. • Шифрование отменено пользователем. • Во время шифрования произошла ошибка. • Все правила шифрования хоста были выполнены. • Шифрование выполняется, на хосте требуется перезагрузка. • На хосте 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.

Левый операнд	Доступные операторы	Правый операнд
		• 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 веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.
- В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
- В веб-интерфейсе KUMA 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** – имя актива.

  Активы, импортированные в KUMA, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить эти имена в веб-интерфейсе KUMA.

- **Тенант** – название тенанта, которому принадлежит актив.
- **Источник актива** – источник информации об активе. Источников может быть несколько: сведения можно добавить в веб-интерфейсе KUMA или с помощью API, а также импортировать из Kaspersky Security Center, KICS/KATA и отчетов MaxPatrol.

  Добавляя в KUMA сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.

- **Создано** – дата и время добавления актива в KUMA.
- **Последнее обновление** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если есть).

  > Если в KUMA 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.

- **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 Kaspersky Security Center.

    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 Kaspersky Security Center.

  - **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 Kaspersky Security Center. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

  - **Идентификатор хоста** – идентификатор *агента администрирования* Kaspersky Security Center, от которого получены сведения об активе. Эта информация доступна для активов, импортированных из Kaspersky Security Center. С помощью этого идентификатора определяется уникальность актива в Kaspersky Security Center.

  - **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 установленной программой 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.

  Эти сведения отображаются, если актив был импортирован из Kaspersky Security Center.

- **Категории** – категории, к которым относится актив (если есть).
- **КИИ категория** – сведения о том, является ли актив объектом критической информационной инфраструктуры (КИИ).

По кнопке **Переместить в группу KSC** вы можете переместить просматриваемый актив между группами администрирования Kaspersky Security Center. 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 Kaspersky Security Center.
- 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 Kaspersky Security Center.

Задачи доступны при интеграции с Kaspersky Security Center и при интеграции с Kaspersky Endpoint Detection and Response.

Добавление активов

Вы можете добавлять в KUMA информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в веб-интерфейсе KUMA или с помощью API. 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.

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center, KICS/KATA и отчетов MaxPatrol.

В процессе добавления активы, уже существующие в KUMA, могут объединяться с добавляемыми активами.

Алгоритм объединения активов:

1. Проверка на уникальность активов в Kaspersky Security Center или KICS/KATA активов:

   - Уникальность актива импортированного из Kaspersky Security Center, проверяется по параметру **Идентификатор хоста**, 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/KATA, определяется по комбинации параметров **IP-адрес**, **IP-адрес сервера KICS/KATA** и **Идентификатор коннектора KICS/KATA**. 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 KUMA содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в KUMA 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
Название	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS/KATA.
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.
Полное доменное имя	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS/KATA. • Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS/KATA. • 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/KATA 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 веб-интерфейсе KUMA.

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 редактировании в веб-интерфейсе KUMA активов, информация о которых получена из Kaspersky Security Center или KICS/KATA, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в веб-интерфейсе KUMA 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.

Объединение дублированных активов

В результате импорта информации об активах из различных источников список активов в KUMA может содержать дубликаты одних и тех же активов. По запросу в Техническую поддержку вы можете получить утилиту для анализа списка активов и объединения дублированных активов.

Добавление информации об активах в веб-интерфейсе KUMA

Чтобы добавить актив в веб-интерфейсе KUMA:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.

2. Введите параметры актива:

   - **Название актива** (обязательно).
   - **Тенант** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN через запятую.
   - **MAC-адрес**.
   - **Владелец**.

3. При необходимости присвойте активу одну или несколько категорий:

   a. Нажмите на кнопку дерева ( ).

   Откроется окно **Выбор категорий**.

b. Установите флажки рядом с категориями, которые следует присвоить активу. С помощью значков плюс (⊞) и минус (⊟) вы можете разворачивать и сворачивать списки категорий.

c. Нажмите **Сохранить**.

Выбранные категории отобразятся в полях **Категории**.

4. При необходимости добавьте в раздел **Программное обеспечение** сведения об операционной системе актива.

5. При необходимости добавьте в раздел **Информация об оборудовании** сведения об оборудовании актива.

6. 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 и уязвимостях активов из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой решения. Вы можете импортировать в KUMA информацию об активах или уязвимостях активов, защищаемых Kaspersky Security Center. Для этого вам нужно предварительно настроить интеграцию между программами.

В параметрах интеграции с Kaspersky Security Center вы можете настроить периодичность автоматического импорта информации об активах, а также при необходимости вы можете импортировать активы вручную по запросу. Запуск импорта по запросу не влияет на время импорта по расписанию. KUMA 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.

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.

По умолчанию информация об основных параметрах активов импортируется каждый час, а информация об атрибутах активов импортируется каждые 12 часов. Информация об атрибутах импортируется только для существующих активов, но не для новых или удаленных.

Если в Kaspersky Security Center зарегистрировано большое количество активов (десятки тысяч хостов), выполнение задачи импорта может занимать значительное время (до 15–20 часов). В процессе импорта могут появляться следующие ошибки:

```
Kaspersky Security Center assets not fetched. Post "https://<KSC
address>:13299/api/v1.0/login": read tcp <KUMA address>:57498-><KSC address>:13299:
read: connection reset by peer
```

```
Kaspersky Security Center assets not fetched. list child: Resource is unavailable
```

```
Kaspersky Security Center assets not fetched. Post "https://<KSC
address>:13299/api/v1.0/login": EOF
```

Чтобы сократить время выполнения импорта и избежать подобных ошибок, необходимо дополнительно настроить параметры интеграции.

Дополнительная настройка параметров интеграции

Для KUMA версии 3.2 и выше можно задать количество хостов, которые будут обрабатываться за один запрос при импорте информации об уязвимостях.

Чтобы задать количество хостов:

1. Создайте файл vuln_iterator_config.json со следующим содержимым:

   ```
   {
   "ksc1.domain.ru": k,
   "ksc2.domain.ru": k
   }
   ```

   где:

   - `ksc1.domain.ru`, `ksc2.domain.ru` – адреса серверов Kaspersky Security Center, указанные в параметрах интеграции KUMA;
   - `k` – число хостов, для которых запрашивается информация об уязвимостях за один запрос. Максимальное количество уязвимостей в одном запросе: 10 000.

2. Разместите созданный файл:

   - Для установки KUMA на одном сервере – в директории /opt/kaspersky/kuma.
   - Для распределенной установки KUMA на нескольких серверах выполните следующую команду на любом контроллере кластера:

     ```
     export POD=$(k0s kubectl get pods --namespace kuma -l "app=core" -o jsonpath="
     {.items[0].metadata.name}");
     k0s kubectl cp --no-preserve -c core ./vuln_iterator_config.json
     kuma/$POD:/opt/kaspersky/kuma/vuln_iterator_config.json
     ```

   Изменения вступят в силу при следующем запуске задачи импорта.

Если при очередном импорте информации из Kaspersky Security Center в KUMA не поступили данные об уже добавленном активе, такой актив помечается архивным. Если в течение следующих 30 дней информация об этом активе так и не поступит, такой актив будет удален.

> KUMA не импортирует активы Kaspersky Security Center, у которых значение параметра **Последнее появление в сети** превышает 30 дней.

При возникновении в Kaspersky Security Center ошибок во время выполнения задач импорта данных KUMA отображает эти ошибки. Если основная информация об активах отсутствует в KUMA во время импорта информации об атрибутах активов (например, активы были удалены во время импорта), то задача завершится без ошибок, но информация об атрибутах этих активов загружена не будет.

В KUMA предусмотрены следующие варианты импорта информации об активах и уязвимостях активов из Kaspersky Security Center:

- **Импорт информации об активах и уязвимостях активов всех Серверов KSC**

  Чтобы импортировать информацию об активах или уязвимостях активов всех Серверов Kaspersky Security Center:

  1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
  2. Импортируйте информацию об активах или уязвимостях активов одним из следующих способов:
     - Если вы хотите импортировать информацию об основных параметрах активов (состоянии защиты, версии антивирусных баз, оборудовании), нажмите на кнопку **Импортировать активы KSC**.
     - Если вы хотите импортировать информацию об остальных параметрах активов (уязвимостях, программном обеспечении, владельцах), нажмите на кнопку **Импортировать атрибуты активов KSC**.
  3. В открывшемся окне выберите тенант, для которого вы хотите выполнить импорт. По умолчанию выбрано значение **Все тенанты** – импорт выполняется для всех тенантов.
  4. Нажмите на кнопку **OK**.

  Информация об активах или уязвимостях активов серверов Kaspersky Security Center будет импортирована в KUMA.

- **Импорт информации об активах и уязвимостях активов отдельного Сервера KSC**

  Чтобы импортировать информацию об активах или уязвимостях активов отдельного Сервера Kaspersky Security Center:

  1. В веб-интерфейсе KUMA перейдите раздел **Параметры** → **Kaspersky Security Center**.

     Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.
  2. Выберите тенант, для которого вы хотите выполнить импорт.

     Откроется окно **Интеграция с Kaspersky Security Center**.
  3. В таблице **Подключения** нажмите на подключение к выбранному Серверу Kaspersky Security Center.

     Откроется окно с параметрами подключения.
  4. Если у Сервера Kaspersky Security Center есть подчиненные Серверы или группы и вы не хотите импортировать информацию об их активах или уязвимостях, выполните следующие действия:
     a. Нажмите на кнопку **Загрузить иерархию**.
     b. Снимите флажки рядом с подчиненными Серверами или группами, для которых вы не хотите выполнять импорт. По умолчанию флажки установлены.
     c. Если вы хотите импортировать информацию об активах или уязвимостях активов новых групп, установите флажок **Импортировать активы из новых групп**. По умолчанию флажок снят.
     d. Нажмите на кнопку **Сохранить**.

5. Импортируйте информацию об активах или уязвимостях активов одним из следующих способов:

   - Если вы хотите импортировать информацию об основных параметрах активов (состоянии защиты, версии антивирусных баз, оборудовании), нажмите на кнопку **Импортировать активы KSC**.

   - Если вы хотите импортировать информацию об остальных параметрах активов (уязвимостях, программном обеспечении, владельцах), нажмите на кнопку **Импортировать атрибуты активов KSC**.

   Информация об активах или уязвимостях активов выбранного Сервера Kaspersky Security Center будет импортирована в KUMA.

Импорт информации об активах из MaxPatrol

Вы можете импортировать в KUMA сведения об активах из системы MaxPatrol.

Вы можете использовать следующие варианты импорта:

- Импорт из отчетов о результатах сканирования сетевых устройств системы MaxPatrol 8.

  Импорт происходит через API с помощью утилиты maxpatrol-tool на сервере, где установлено Ядро KUMA. Утилита входит в комплект поставки KUMA и расположена в архиве установщика в директории /kuma-ansible-installer/roles/kuma/files.

- Импорт данных из системы MaxPatrol VM.

  Импорт происходит через API с помощью утилиты kuma_ptvm. Утилита входит в комплект поставки KUMA и расположена в архиве установщика в директории /kuma-ansible-installer/roles/kuma/files.

Импортированные активы отображаются в веб-интерфейсе KUMA в разделе **Активы**. При необходимости вы можете редактировать параметры активов.

Импорт данных из отчетов MaxPatrol

Импорт данных об активах из отчета поддерживается для MaxPatrol 8.

Чтобы импортировать данные об активах из отчета MaxPatrol:

1. Сформируйте в MaxPatrol отчет сканирования сетевых активов в формате **XML file** и скопируйте файл отчета на сервер Ядра KUMA. Подробнее о задачах на сканирование и форматах выходных файлов см. в документации MaxPatrol.

   Импорт данных из отчетов в формате **SIEM integration file** не поддерживается. Требуется выбрать формат **XML file**.

2. Создайте файл с токеном для доступа к KUMA REST API. Для удобства рекомендуется разместить его в папке отчета MaxPatrol. Файл не должен содержать ничего, кроме токена.

   Требования к учетным записям, для которых генерируется API-токен:

   - Роль Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня.

   - Доступ к тенанту, в который будут импортированы активы.

- Настроены права на использование API-запросов GET /api/v3/users/whoami и POST /api/v3/assets/import.

> Мы рекомендуем для импорта активов из MaxPatrol создать отдельного пользователя с минимально необходимым набором прав на использование API-запросов.

3. Скопируйте утилиту maxpatrol-tool на сервер с Ядром KUMA и сделайте файл утилиты исполняемым с помощью команды:

   ```
   chmod +x <путь до файла maxpatrol-tool на сервере с Ядром KUMA>
   ```

4. Запустите утилиту maxpatrol-tool:

   ```
   ./maxpatrol-tool --kuma-rest <адрес и порт сервера KUMA REST API> --token <путь и имя файла с API-токеном> --tenant <название тенанта, куда будут помещены активы> <путь и имя файла с отчетом MaxPatrol> --cert <путь к файлу сертификата Ядра KUMA>
   ```

   Сертификат Ядра можно скачать в веб-интерфейсе KUMA.

   Пример: `./maxpatrol-tool --kuma-rest kuma.example.com:7223 --token token.txt --tenant Main example.xml --cert /tmp/ca.cert`

   Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения полного отчета о полученных активах `--verbose, -v`. Подробное описание доступных флагов и команд приведено в таблице Флаги и команды утилиты maxpatrol-tool. Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета MaxPatrol в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

```
Пример:
inserted 2 assets;
updated 1 assets;
errors occurred: []
```

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. Сведения об ошибках отображаются при использовании флага `--verbose`.
- Если в одном отчете MaxPatrol есть активы с одинаковыми IP-адресами и полными именами домена (FQDN), эти активы объединяются. Сведения об их уязвимостях и программном обеспечении также объединяются в одном активе.

  > При загрузке активов из MaxPatrol активы с аналогичными IP-адресами и полными именами доменов (FQDN), ранее импортированные из Kaspersky Security Center, перезаписываются.

  Чтобы этого избежать, вам требуется настроить фильтрацию активов по диапазону с помощью команды:

  `--ignore <диапазоны IP-адресов>` или `-i <диапазоны IP-адресов>`

  Активы, соответствующие условиям фильтрации, не загружаются. Описание команды вы можете просмотреть в таблице *Флаги и команды утилиты maxpatrol-tool*.

Флаги и команды утилиты maxpatrol-tool

Флаги и команды	Описание
`--kuma-rest < адрес и порт сервера KUMA REST API >, -a < адрес и порт сервера KUMA REST API >`	Адрес сервера с Ядром KUMA, куда будет производиться импорт активов, с указанием порта. Например, `kuma.example.com:7223`. По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token < путь и имя файла с API-токеном >, -t <путь и имя файла с API-токеном>`	Путь и имя файла, содержащее токен для доступа к REST API. Файл должен содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Главного администратора, Администратора тенанта, Администратора второго уровня или Администратора первого уровня.
`--tenant <название тенанта>, -T <название тенанта>`	Название тенанта KUMA, в который будут импортированы активы из отчета MaxPatrol.
`--dns <диапазоны IP-адресов> или -d <диапазоны IP-адресов>`	Используется для обогащения IP-адресов FQDN из указанных диапазонов с помощью DNS, если для этих адресов FQDN не был указан. Пример: `--dns 0.0.0.0-9.255.255.255,11.0.0.0-255.255.255,10.0.0.2`
`--dns-server <IP-адрес DNS-сервера>, -s <IP-адрес DNS-сервера>`	Адрес DNS-сервера, к которому должна обращаться утилита для получения информации о FQDN. Пример: `--dns-server 8.8.8.8`
`--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`	Диапазоны адресов активов, которые при импорте следует пропустить. Пример: `--ignore 8.8.0.0-8.8.255.255, 10.10.0.1`
`--verbose, -v`	Выведение полного отчета о полученных активах и ошибках, возникших в процессе импорта.

`--help, -h`
`help`
	Получение справочной информации об утилите или команде.
	Примеры:
	`./maxpatrol-tool help`
	`./maxpatrol-tool <команда> --help`

`version`	Получение информации о версии утилиты maxpatrol-tool.
`completion`	Создание скрипта автозавершения для указанной оболочки.
`--cert <путь до файла с сертификатом Ядра KUMA>`	Путь к сертификату Ядра KUMA.

Примеры:

- `./maxpatrol-tool --kuma-rest kuma.example.com:7223 --token token.txt --tenant Main example.xml --cert /example-directory/ca.cert` – импорт активов в KUMA из отчета MaxPatrol example.xml.
- `./maxpatrol-tool help` – получение справки об утилите.

Возможные ошибки

Сообщение об ошибке	Описание
must provide path to xml file to import assets	Не указан путь к файлу отчета MaxPatrol.
incorrect IP address format	Некорректный формат IP-адреса. Может возникнуть при указании некорректных диапазонов IP.
no tenants match specified name	Для указанного названия тенанта не было найдено подходящих тенантов с помощью REST API.
unexpected number of tenants (%v) match specified name. Tenants are: %v	Из KUMA вернулось больше одного тенанта для указанного названия тенанта.
could not parse file due to error: %w	Ошибка чтения xml-файла с отчетом MaxPatrol.
error decoding token: %w	Ошибка чтения файла с API-токеном.

Сообщение об ошибке	Описание
error when importing files to KUMA: %w	Ошибка передачи сведений об активах в KUMA.
skipped asset with no FQDN and IP address	У одного из активов в отчете не было FQDN и IP-адреса. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid FQDN: %v	У одного из активов в отчете был некорректный FQDN. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid IP address: %v	У одного из активов в отчете был некорректный IP-адрес. Сведения об этом активе не были отправлены в KUMA.
KUMA response: %v	При импорте сведений об активах произошла ошибка с указанным ответом.
unexpected status code %v	При импорте сведений об активах от KUMA был получен неожиданный код HTTP.

Импорт данных об активах из MaxPatrol VM

В поставку KUMA входит утилита kuma-ptvm, которая состоит из исполняемого файла и файла конфигурации. Поддерживается работа под управлением ОС Windows и Linux. Утилита позволяет выполнить подключение к API MaxPatrol VM, получить данные об устройствах и их атрибутах, включая уязвимости, а также позволяет отредактировать данные об активах и импортировать данные с использованием API KUMA. Импорт данных поддерживается для версий MaxPatrol VM 1.1–2.7 включительно.

Настройка импорта информации об активах из MaxPatrol VM в KUMA состоит из следующих шагов:

1. Подготовительные действия в KUMA и MaxPatrol VM.

   Вам потребуется создать учетные записи пользователей и токен KUMA для операций через API.

2. Создание файла конфигурации с параметрами экспорта и импорта данных.

3. Импорт данных об активах в KUMA с помощью утилиты kuma-ptvm:

   a. Данные экспортируются из MaxPatrol VM и сохраняются в директории утилиты. Информация по каждому тенанту сохраняется в отдельный файл в формате JSON.

      При необходимости вы можете отредактировать полученные файлы.

   b. Информация из файлов импортируется в KUMA.

При повторном импорте уже существующие в KUMA активы будут перезаписаны. Таким образом устраненные уязвимости будут удалены.

Известные ограничения

Если для двух активов с разными FQDN указан один IP-адрес, KUMA импортирует такие активы как два разных актива, активы не будут объединены.

Если у актива два ПО с одинаковыми данными в полях name, version, vendor, KUMA импортирует эти данные как одно ПО, несмотря на разные пути установки ПО в активе.

Если в конфигурационном файле kuma-ptvm-config.yaml вы укажете параметр strict_import со значением false, то из MaxPatrol будут импортированы данные по всем активам, в том числе без обязательных для KUMA полей и с недопустимыми для KUMA значениями полей. Если FQDN актива содержит пробел или "_", данные по таким активам не будут импортированы в KUMA, в журнале будет указано, что такие активы пропущены при импорте.

Если при импорте происходит ошибка, информация об ошибке регистрируется в журнале и выполнение импорта прекращается.

Подготовительные действия

1. Создайте отдельную учетную запись пользователя в KUMA и в MaxPatrol VM с минимально необходимым набором прав на использование API-запросов.

2. Создайте учетные записи, для которых впоследствии сгенерируете API-токен.

   Требования к учетным записям, для которых генерируется API-токен:

   - Роль Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня.

   - Доступ к тенанту, в который будут импортированы активы.

   - В учетной записи пользователя в группе параметров **Права доступа через API** установлен флажок для POST /api/v3/assets/import.

3. Сгенерируйте токен для доступа к KUMA REST API.

Создание конфигурационного файла

Чтобы создать конфигурационный файл:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer/roles/kuma/files/
   ```

2. Распакуйте архив kuma-ptvm.tar.gz, выполнив следующую команду:

   ```
   tar -xvf kuma-ptvm.tar.gz
   ```

3. Скопируйте шаблон kuma-ptvm-config-template.yaml и создайте конфигурационный файл с именем kuma-ptvm-config.yaml:

   ```
   cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
   ```

4. Отредактируйте параметры конфигурационного файла kuma-ptvm-config.yaml.

5. Сохраните изменения в файле.

Конфигурационный файл будет создан. Теперь вы можете переходить к шагу Импорт информации об активах.

Импорт данных об активах

Чтобы импортировать данные об активах:

1. Если вы хотите импортировать информацию об активах из MaxPatrol VM в KUMA без промежуточной проверки экспортированных данных, запустите утилиту kuma-ptvm со следующими параметрами:

   ```
   ./kuma-ptvm --config <путь к файлу kuma-ptvm-config.yaml> --download --upload
   ```

2. Если вы хотите проверить правильность экспортированных из MaxPatrol VM данных перед импортом в KUMA, выполните следующие действия:

   a. Запустите утилиту kuma-ptvm со следующими параметрами:

   ```
   ./kuma-ptvm --config <путь к файлу kuma-ptvm-config.yaml> --download
   ```

   При необходимости вы можете использовать параметр `--cvss-version <номер CVSS версии>`, чтобы указать, для какой версии CVSS нужно загрузить значения уязвимостей активов. Доступные значения:

   - `2` – загружаются только значения CVSS версии 2.
   - `3` – загружаются только значения CVSS версии 3. Если уязвимость описана только по версии 2, поле CVSS будет пустым.
   - `latest` – загружаются значения последней доступной версии CVSS (значение по умолчанию). Если уязвимость не имеет значения CVSS версии 3, используется значение версии 2.

   Примеры:

   ```
   ./kuma-ptvm --config kuma-ptvm-config.yaml --cvss-version 2 --download
   ./kuma-ptvm --config kuma-ptvm-config.yaml --cvss-version 3 --download
   ./kuma-ptvm --config kuma-ptvm-config.yaml --cvss-version latest --download
   ```

   Для каждого тенанта, указанного в конфигурационном файле, будет создан отдельный файл с именем вида <Идентификатор тенанта KUMA>.JSON. Также при экспорте будет создан файл tenants со списком JSON-файлов для загрузки в KUMA. Все файлы сохраняются в директории утилиты.

   b. Проверьте экспортированные файлы активов и при необходимости внесите изменения:

   - Распределите активы по соответствующим тенантам.
   - Из файла тенанта по умолчанию default вручную перенесите данные активов в файлы нужных тенантов.
   - В файле tenants отредактируйте список тенантов, активы которых будут импортированы в KUMA.

   c. Импортируйте информацию об активах в KUMA с помощью команды:

   ```
   ./kuma-ptvm --config <путь к файлу kuma-ptvm-config.yaml> --upload
   ```

   Чтобы просмотреть информацию о доступных командах утилиты, выполните команду --help.

Информация об активах будет импортирована из MaxPatrol VM в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Возможные ошибки

При запуске утилиты kuma-ptvm может вернуться ошибка `tls: failed to verify certificate: x509: certificate is valid for localhost`.

Решение:

- Выписать сертификат в соответствии с документацией MaxPatrol. Мы рекомендуем этот способ устранения ошибки, как предпочтительный.
- Отключить проверку сертификата.

Чтобы отключить проверку сертификата, добавьте в конфигурационный файл в разделе MaxPatrol settings следующую строку:

```
ignore_server_cert: true
```

В результате запуск утилиты выполняется без ошибок.

Параметры конфигурационного файла kuma–ptvm–config.yaml

В таблице представлены параметры, доступные для настройки в файле kuma-ptvm-config.yaml.

Описание параметров конфигурационного файла kuma-ptvm-config.yaml

Параметр	Описание	Значения
`log_level`	Необязательный параметр в секции `General settings`. Уровень журналирования.	Доступные значения: • `trace` • `info` • `warning` • `error` Значение по умолчанию: `info`.
`period`	Необязательный параметр в секции `General settings`. Из MaxPatrol будут экспортированы данные об активах, которые изменялись за указанный срок.	Ограничения отсутствуют. Значение по умолчанию: `30d`.
`strict_import`	Необязательный параметр в секции `General settings`. При экспорте активов из MaxPatrol проверять, заполнены ли обязательные для KUMA поля. Не экспортировать из MaxPatrol активы, не прошедшие проверку.	Доступные значения: • `true` – проверять наличие обязательных для KUMA полей. • `false` – не проверять наличие обязательных для KUMA полей. Значение по умолчанию: `false`. Мы рекомендуем указывать значение `true` при экспорте активов из MaxPatrol, это позволит выявить возможные ошибки в файлах JSON и исправить ошибки перед тем, как вы импортируете активы в KUMA.
`parallel_downloading`	Необязательный параметр в секции `General settings`. Определяет режим загрузки при импорте данных из MaxPatrol.	Доступные значения: • `false` – загружать CSV-файлы параллельно. • `false` – загружать CSV-файлы последовательно, чтобы снизить нагрузку на MaxPatrol. Значение по умолчанию: `true`. Мы рекомендуем указывать значение `false`, если необходимо уменьшить нагрузку на MaxPatrol во время импорта данных.
`endpoint`	Обязательный параметр в секции `KUMA settings`. URL сервера KUMA API. Например: kuma.example.com:7223	–
`token`	Обязательный параметр в секции `KUMA settings`. Токен KUMA API.	–
`ignore_server_cert`	Необязательный параметр в секции `KUMA settings`. Проверка сертификата KUMA.	Доступные значения: • `true` – отключить проверку сертификата KUMA. • `false` – выполнить проверку сертификата KUMA. Параметр не включен в шаблон конфигурационного файла. Вы можете указать параметр со значением true вручную, тогда при запуске утилита kuma–ptvm не будет проверять сертификат.
`endpoint`	Обязательный параметр в секции `MaxPatrol VM settings`. URL сервера MaxPatrol API.	–
`user`	Обязательный параметр в секции `MaxPatrol VM settings`. Имя пользователя MaxPatrol API.	–

Параметр	Описание	Значения
`password`	Обязательный параметр в секции `MaxPatrol VM settings`. Пароль пользователя MaxPatrol API.	–
`secret`	Обязательный параметр в секции `MaxPatrol VM settings`. Секрет MaxPatrol API	–
`ignore_server_cert`	Необязательный параметр в секции `MaxPatrol VM settings`. Проверка сертификата MaxPatrol.	Доступные значения: • `true` – отключить проверку сертификата MaxPatrol. • `false` – выполнить проверку сертификата MaxPatrol. Параметр не включен в шаблон конфигурационного файла. Вы можете указать параметр со значением true вручную, в случае возникновения ошибки `tls: failed to verify certificate: x509: certificate is valid for localhost`. В таком случае при запуске утилита kuma-ptvm не будет проверять сертификат. Мы рекомендуем выписать сертификат в соответствии с документацией MaxPatrol, как предпочтительный способ устранения ошибки.
`only_exploitable`	Необязательный параметр в секции `Vulnerability filter`. Экспортировать из MaxPatrol только активы с уязвимостями, для которых известны эксплойты.	Доступные значения: • `true` – экспортировать только активы с уязвимостями, для которых известны эксплойты. • `false` – экспортировать все активы. Значение по умолчанию: `false`.
`min_severity`	Необязательный параметр в секции `Vulnerability filter`. Импортировать только уязвимости указанного уровня и выше.	Доступные значения: • `low` • `medium` • `high` • `critical` Значение по умолчанию: `low`.
`id`	Обязательный параметр в секции `Tenant map`. Идентификатор тенанта в KUMA. Активы распределяются по тенантам в том порядке, в каком тенанты указаны в конфигурационном файле: чем выше тенант в списке, тем выше у него приоритет. Таким образом вы можете указывать и перекрывающиеся подсети.	–
`fqdn`	Необязательный параметр в секции `Tenant map`. Регулярное выражение для поиска FQDN актива.	–
`networks`	Необязательный параметр в секции `Tenant map`. Одна или несколько подсетей.	–
`default_tenant`	Необязательный параметр. Идентификатор тенанта KUMA по умолчанию, куда будут поступать данные об активах, которые не удалось распределить по тенантам, заданным в секции параметров Tenants.	–

Импорт информации об активах из KICS for Networks

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 запустить задачу на обновление данных об активах for Networks для тенанта:

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **KICS/KATA**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с KICS/KATA**.
3. Нажмите на кнопку **Импортировать активы**.

   В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача на получение данных об учетных записях выбранного тенанта.

Примеры сравнения полей активов при импорте

Каждый импортируемый актив сравнивается с активом KUMA.

Проверка на совпадение значений в полях IP, MAC, FQDN по двум полям

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Заполнено	Заполнено	Не заполнено
Импортируемый актив 1	Заполнено, совпадает	Заполнено, совпадает	Заполнено
Импортируемый актив 2	Заполнено, совпадает	Заполнено, совпадает	Не заполнено
Импортируемый актив 3	Заполнено, совпадает	Не заполнено	Заполнено
Импортируемый актив 4	Не заполнено	Заполнено, совпадает	Заполнено
Импортируемый актив 5	Заполнено, совпадает	Не заполнено	Не заполнено
Импортируемый актив 6	Не заполнено	Не заполнено	Заполнено

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP, по полю MAC нет противоречия. Активы будут объединены.
- Импортируемый актив 2 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP. Активы будут объединены.
- Импортируемый актив 3 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и MAC, по полю IP нет противоречия. Активы будут объединены.
- Импортируемый актив 4 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.
- Импортируемый актив 5 и актив KUMA: для обоих активов заполнено и совпадает поле FQDN, по полям IP и MAC нет противоречия. Активы будут объединены.
- Импортируемый актив 6 и актив KUMA: 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 KUMA	Не заполнено	Заполнено	Не заполнено
Импортируемый актив 1	Заполнено	Заполнено, совпадает	Заполнено
Импортируемый актив 2	Заполнено	Заполнено, совпадает	Не заполнено
Импортируемый актив 3	Заполнено	Не заполнено	Заполнено
Импортируемый актив 4	Не заполнено	Не заполнено	Заполнено

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.
- Импортируемый актив 2 и актив KUMA: заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.
- Импортируемый актив 3 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.
- Импортируемый актив 4 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

Назначение активу категории

Чтобы назначить категорию одному активу:

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив.
4. В открывшемся окне нажмите на кнопку **Изменить**.
5. В поле **Категории** нажмите на кнопку .
6. Выберите категорию.

   Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку .
7. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Чтобы назначить категорию нескольким активам:

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите 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 **Сохранить**.

Категория будет назначена.

Не назначайте активам категорию `Categorized assets`.

Привязка группы активов к категории

Чтобы привязать группу активов к категории:

1. В разделе **Активы** веб-интерфейса KUMA в шапке 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 KUMA 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 разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.
2. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

3. Внесите необходимые изменения в доступные поля:

- **Название актива** (обязательно). Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS/KATA.
- **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN через запятую.
- **MAC-адрес**
- **Владелец**
- **Информация о программном обеспечении**:
  - **Название ОС**
  - **Версия 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 ссылки **Добавить процессор**.

  Доступные поля для описания диска актива:

  - **Свободных байт на диске**
  - **Объем диска**

    Активу можно добавить диски с помощью ссылки **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 ссылки **Добавить сетевую карту**.

- Настраиваемые поля.
- Категория КИИ.

4. Назначьте или измените активу категорию:

   a. Нажмите на кнопку дерева ( ).

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу.

   c. Нажмите **Сохранить**.

   Выбранные категории отобразятся в полях **Категории**.

   Кроме того, можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

   Не назначайте активам категорию `Categorized assets`.

5. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Архивирование активов

В KUMA функция архивирования доступна для следующих типов активов:

- Для активов, импортированных из Kaspersky Security Center и KICS.

  Если после десяти попыток импорта KUMA 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 параметра по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно. Архивный актив станет активным, если KUMA получит информацию об активе от источника до истечения срока хранения архивных активов.

- Для объединенных активов.

  При импорте KUMA 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 веб-интерфейсе или с помощью API, не архивируются.

Актив становится архивным при следующих условиях:

- KUMA не получила информацию об активе от Kaspersky Security Center или KICS/KATA 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**.

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/KATA.
- Соединение с сервером Kaspersky Security Center отсутствует больше 30 дней.

Архивные активы, участвующие в динамической категоризации, остаются архивными. Архивному активу может быть назначена или изменена категория КИИ. При этом если актив оказался в алерте или инциденте, у алерта или инцидента также изменится категория КИИ, что может повлиять на видимость алерта или инцидента для пользователей с ограничением доступа к КИИ.

Чтобы настроить срок хранения архивных активов:

1. В веб-интерфейсе KUMA выберите раздел **Параметры** → **Активы**.

   Отобразится окно **Активы**.

2. Введите в поле **Срок хранения архивных активов** желаемое значение.

   Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно

3. Нажмите **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 веб-интерфейсе KUMA 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

Если вам больше не нужно получать информацию от актива или информация об активе долгое время не обновлялась, в KUMA есть возможность удаления активов. Возможность удаления доступна для главного администратора, администратора тенанта, аналитиков второго и первого уровней. Если после удаления актива в KUMA сведения о нем начнут поступать из Kaspersky Security Center, KUMA создаст актив с новым идентификатором.

В KUMA доступны следующие способы удаления активов:

- Автоматически.

  KUMA автоматически удаляет только архивные активы. KUMA удалит архивный актив, если информация об активе не обновлялась больше срока хранения архивных активов.

- Вручную.

Чтобы удалить актив вручную:

1. В веб-интерфейсе KUMA → **Активы** нажмите на актив, который вы хотите удалить.

   В правой части веб-интерфейса откроется окно **Информация об активе**.

2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

3. Нажмите **OK**.

Актив будет удален и больше не будет отображаться в карточке алерта или в карточке инцидента.

Массовое удаление активов

В веб-интерфейсе KUMA вы можете осуществить множественный выбор активов с помощью фильтра и удалить все выбранные активы.

Для удаления активов вы должны обладать правами на удаление активов.

Массовое удаление активов

Чтобы удалить все выбранные активы:

1. В разделе **Активы** веб-интерфейса KUMA 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 решения), а затем удалить папку.

Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять программы сторонних производителей, в том числе программы Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих программ.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Программа – 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 важности равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень важности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем важности 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 программ сторонних производителей и закрыть уязвимости на активах в KUMA.

Чтобы установить обновления и закрыть уязвимости программ сторонних производителей на активе в KUMA:

1. Откройте окно информации об активе одним из следующих способов:

   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.

   - В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.

   - В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий → выберите требуемое событие → нажмите на ссылку 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 программами, 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, в веб-интерфейсе KUMA нажмите на кнопку **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 подчиненных серверов 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 KUMA при загрузке иерархии во время импорта активов из Kaspersky Security Center. Предварительно вам требуется настроить интеграцию KUMA с Kaspersky Security Center.

Чтобы переместить один актив в выбранную группу администрирования:

1. Откройте окно информации об активе одним из следующих способов:
   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.
   - В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
2. В окне информации об активе нажмите на кнопку **Переместить в группу KSC**.
3. Нажмите на кнопку **Переместить в группу KSC**.
4. В открывшемся окне выберите группу.

   Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.
5. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

Чтобы переместить несколько активов в выбранную группу администрирования:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.
2. Выберите категорию с требуемыми активами.
3. Установите флажки рядом с активами, которые хотите переместить в группу.
4. Нажмите на кнопку **Переместить в группу KSC**.

   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 KUMA 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 KUMA эти сведения еще не отображаются. При попытке переместить такой актив в группу администрирования, в которой он уже находится, KUMA возвращает ошибку **Не удалось переместить активы в другую группу KSC**.

Аудит активов

В KUMA можно настроить создание событий аудита активов при следующих условиях:

- Актив добавлен в KUMA. Отслеживается создание актива вручную, а также создание при импорте через REST API, импорте из Kaspersky Security Center или KICS/KATA.

- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:

  - Name

  - IP address

  - Mac Address

  - FQDN

  - Operating system

  Изменения полей может происходить при обновлении актива во время импорта.

- Актив удален из KUMA. Отслеживается удаление активов вручную, а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS/KATA, 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/KATA.

- 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 в KUMA создаются 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. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA.

2. Выполните одно из действий с тенантом, для которого вы хотите настроить аудит активов:

   - Добавьте тенант с помощью кнопки **Добавить тенант**, если аудит активов для требуемого тенанта настраивается впервые.

     В открывшемся окне **Аудит активов** выберите имя для нового тенанта.

   - Выберите существующий тенант в таблице, если аудит активов для требуемого тенанта уже был настроен.

     В открывшемся окне **Аудит активов** имя тенанта уже задано и редактировать его нельзя.

   - Клонируйте настройки существующего тенанта, чтобы создать копию конфигурации условий для тенанта, для которого вы хотите настроить аудит активов впервые. Для этого установите флажок напротив тенанта, конфигурацию которого требуется копировать, и нажмите **Клонировать**. В открывшемся окне **Аудит активов** выберите имя тенанта, в котором будет использована конфигурация исходного тенанта.

3. 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 решения.

      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 новую точку назначения.

      При создании новой точки назначения заполните параметры, как указано в описании точки назначения.

   c. Нажмите **Сохранить**.

Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения.

4. Нажмите **Сохранить**.

Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Нажмите **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	`Kaspersky`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Включение и выключение аудита активов

Можно включить или выключить аудит активов для тенанта:

Чтобы включить или выключить аудит активов для тенанта:

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого вы хотите включить или выключить аудит активов.

   Откроется окно **Аудит активов**.

2. Установите или снимите в верхней части окна флажок **Выключено**.

3. Нажмите **Сохранить**.

По умолчанию при включенном аудите активов в KUMA 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. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого вы хотите включить или выключить условие создания событий аудита активов.

   Откроется окно **Аудит активов**.

2. Установите или снимите напротив нужных условий флажок **Выключено**.

3. Нажмите **Сохранить**.

Для условий с установленным флажком **Выключено** будут создаваться только события аудита, а базовые события создаваться не будут.

Обнаружение неизвестных активов

На основе обрабатываемых событий KUMA позволяет вам обнаруживать в инфраструктуре неизвестные активы, которые не входят в список уже добавленных активов KUMA. Актив при этом должен иметь IP-адрес или имя хоста. Обнаружение неизвестного актива может свидетельствовать как о штатной ситуации, так и об инциденте информационной безопасности.

Для обнаружения неизвестных активов используются следующие предустановленные правила корреляции:

- [OOTB][Net] Detection unknown assets in device fields.
- [OOTB][Net] Detection unknown assets in source fields.
- [OOTB][Net] Detection unknown assets in destination fields.

В этих правилах корреляции используются фильтры для настройки контролируемого сетевого сегмента и фильтры исключений. С помощью фильтров вы можете настроить логику срабатывания правил, подходящую именно вашей сетевой инфраструктуре. В результате срабатывания правил обнаруженные неизвестные активы будут добавлены в активный лист [OOTB][Net] Detection unknown assets.

Запись об обнаруженном активе хранится в активном листе [OOTB][Net] Detection unknown assets в течение 7 дней. При повторном срабатывании какого-либо из правил, дублирующая запись об уже добавленном активе в активный лист не вносится.

Правила корреляции, фильтры и активный лист предустановлены. Вы также можете импортировать эти ресурсы из репозитория.

Правила корреляции

[OOTB][Net] Detection unknown assets in device fields

Правило анализирует данные в полях DeviceAddress и DeviceHostName событий. Если IP-адрес или имя хоста из этих полей отсутствует в списке активов KUMA, то правило сработает.

При этом должны выполняться следующие условия:

- Актив не входит в фильтр исключений [OOTB][Net] Exceptions from the device addresses.
- IP-адрес принадлежит подсети, указанной в фильтре [OOTB][Net] Controlled network device.

[OOTB][Net] Detection unknown assets in source fields

Правило анализирует данные в полях SourceAddress и SourceHostName событий. Если IP-адрес или имя хоста из этих полей отсутствует в списке активов KUMA, то правило сработает.

При этом должны выполняться следующие условия:

- Актив не входит в фильтр исключений [OOTB][Net] Exceptions from the source addresses.
- IP-адрес принадлежит подсети, указанной в [OOTB][Net] Controlled network source.

[OOTB][Net] Detection unknown assets in destination fields

Правило анализирует данные в полях DestinationAddress и DestinationHostName событий. Если IP-адрес или имя хоста из этих полей отсутствует в списке активов KUMA, то правило сработает.

При этом должны выполняться следующие условия:

- Актив не входит в фильтр исключений [OOTB][Net] Exceptions from the destination addresses.
- IP-адрес принадлежит подсети, указанной в [OOTB][Net] Controlled network destination.

Фильтры

Фильтры исключений

Фильтры исключений содержат списки IP-адресов и имен хостов активов, при обнаружении которых правила корреляции срабатывать не будут. Добавьте IP-адреса и имена хостов в фильтры исключений перед использованием правил корреляции. Для корректной работы правил фильтры не должны быть пустыми.

К фильтрам исключений относятся:

- [OOTB][Net] Exceptions from the device addresses.
- [OOTB][Net] Exceptions from the source addresses.
- [OOTB][Net] Exceptions from the destination addresses.

Фильтры исключений расположены в каталоге OOTB/Integration.

Фильтры контролируемых подсетей

Фильтры подсетей содержат списки подсетей, в которых правила корреляции отслеживают появление новых активов. Добавьте подсети в фильтры перед использованием правил корреляции. Без списка подсетей правила корреляции срабатывать не будут.

К фильтрам подсетей относятся:

- [OOTB][Net] Controlled network device.
- [OOTB][Net] Controlled network source.
- [OOTB][Net] Controlled network destination.

Фильтры подсетей расположены в каталоге OOTB/Integration.

Настройка обнаружения неизвестных активов в вашей сети

Чтобы настроить обнаружение неизвестных активов:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Фильтры**.

2. В списке фильтров последовательно выберите каждый из следующих фильтров и укажите IP-адреса или имена хостов, которые хотите исключить из правил корреляции:

   - [OOTB][Net] Exceptions from the device addresses.

   - [OOTB][Net] Exceptions from the source addresses.

   - [OOTB][Net] Exceptions from the destination addresses.

3. В списке фильтров последовательно выберите каждый из следующих фильтров и укажите подсети, в которых следует искать неизвестные активы:

   - [OOTB][Net] Controlled network device.

   - [OOTB][Net] Controlled network source.

   - [OOTB][Net] Controlled network destination.

   Обнаружение неизвестных активов в указанных вами подсетях настроено. Информация об обнаруженных активах будет добавляться в активный лист [OOTB][Net] Detection unknown assets.

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 веб-интерфейсе KUMA в разделе **Параметры** → **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, которому должно соответствовать значение, записываемое в поле.

Чтобы создать настраиваемое поле активов:

1. В разделе веб-интерфейса KUMA **Параметры** → **Активы** нажмите на кнопку **Добавить поле**.

   В таблице **Настраиваемые поля** добавится пустая строка. Вы можете добавить сразу несколько строк с параметрами настраиваемого поля.

2. Заполните столбцы с параметрами настраиваемого поля:

   - **Название** (обязательно) – от 1 до 128 символов в кодировке Unicode.
   - **Значение по умолчанию** – от 1 до 1024 символов в кодировке Unicode.
   - **Маска** – от 1 до 1024 символов в кодировке Unicode.

3. Нажмите **Сохранить**.

К модели данных активов добавлено настраиваемое поле.

Чтобы удалить или изменить настраиваемое поле активов:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Активы**.
2. Сделайте необходимые изменения в таблице **Настраиваемые поля**:

   - Вы можете удалить настраиваемые поля, нажав на значок ✕ напротив строки с параметрами нужного поля. 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.
   - Измените порядок отображения полей, перетягивая строки мышью за значок ⠿.

3. Нажмите **Сохранить**.

Изменения внесены.

Активы критической информационной инфраструктуры

В KUMA можно помечать активы, относящиеся к критической информационной инфраструктуре (КИИ) Российской Федерации. Это позволяет ограничивать возможности пользователей KUMA по обращению с алертами и инцидентами, к которым относятся активы, относящиеся к объектам КИИ.

Присваивать активам КИИ-категорию можно, если в KUMA действует лицензия с модулем GosSOPKA.

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 веб-интерфейсе KUMA в разделе **Активы** выберите нужный актив.

   Откроется окно **Информация об активе**.

2. 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**.

3. Нажмите **Сохранить**.

Интеграция с другими решениями

В этом разделе описано, как интегрировать KUMA с другими приложениями для расширения возможностей решения.

Интеграция с Kaspersky Security Center

KUMA можно интегрировать с Kaspersky Security Center Windows или с Kaspersky Security Center Linux. Далее под Kaspersky Security Center подразумевается то приложение, которое вы выбрали для интеграции.

Вы можете настроить интеграцию с выбранными серверами Kaspersky Security Center для одного, нескольких или всех тенантов KUMA. Если интеграция с Kaspersky Security Center включена, вы можете импортировать информацию об активах, защищаемых этой программой, управлять активами с помощью задач, а также импортировать события из базы событий Kaspersky Security Center.

> Предварительно вам требуется убедиться, что на требуемом сервере Kaspersky Security Center разрешено входящее соединение для сервера с KUMA.

Настройка интеграции KUMA с Kaspersky Security Center включает следующие этапы:

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.

Секрет (учетная роль в Kaspersky Security Center) для интеграции KUMA с Kaspersky Security Center следует создавать с учетом специфики иерархии Сервера Администрирования (наличие виртуальных серверов, особенности администрирования сервера и т.д.), типов устройств, которыми будет управлять Сервер Администрирования (ОС, тип: сервера, мобильные устройства и т.д.). Все эти нюансы регулируются и настраиваются на стороне Kaspersky Security Center.

Список действий, которые можно совершать в KUMA над активами из Kaspersky Security Center:

- Запуск задачи типа **Обновление**.
- Запуск задачи типа **Поиск вирусов**.
- Перемещение активов по группам Kaspersky Security Center.
- Принятие обновлений ПО (для устранения уязвимости на активе в Kaspersky Security Center).

Чтобы иметь возможность осуществить вышеперечисленные действия, можно использовать предустановленную учетную запись в Kaspersky Security Center с ролью Главный администратор. В таком случае не нужно будет добавлять вручную дополнительные разрешения.

Также вы можете использовать предустановленную роль в Kaspersky Security Center - "Администратор Kaspersky Endpoint Security", при этом необходимо дополнительно проставить доступ к следующим функциям:

1. Управление группами администрирования.
2. Системное администрирование.

   Могут понадобиться какие-то дополнительные разрешения, исходя из конфигурации Kaspersky Security Center.

Минимальные разрешения для интеграции с Kaspersky Security Center:

- Access objects regardless of their ACLs – позволяет импортировать активы Kaspersky Security Center в KUMA.

- Management of administration groups – позволяет перемещать активы между группами в Kaspersky Security Center из интерфейса KUMA.

- Basic functionality – позволяет создавать и запускать задачи на хостах под управлением Kaspersky Endpoint Security.

Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. **Добавление созданной учетной записи в список исключений двухфакторной аутентификации**

   В Консоли администрирования Kaspersky Security Center исключите учетную запись, созданную для интеграции KUMA с Kaspersky Security Center, из двухфакторной аутентификации в Kaspersky Security Center Windows или Kaspersky Security Center Linux.

3. **Создание секрета с типом credentials для соединения с Kaspersky Security Center**

4. **Настройка параметров интеграции с Kaspersky Security Center**

5. **Создание подключения к серверу Kaspersky Security Center для импорта информации об активах**

   Если вы хотите импортировать в KUMA информацию об активах, зарегистрированных на серверах Kaspersky Security Center, вам требуется создать отдельное подключение к каждому серверу Kaspersky Security Center для каждого выбранного тенанта.

   Если для тенанта выключена интеграция или отсутствует подключение к Kaspersky Security Center, при попытке импорта информации об активах в веб-интерфейсе KUMA отобразится ошибка. Процесс импорта при этом не запускается.

https://rutube.ru/video/c3012fb60209d69c7adedfefaaf93535/

Настройка параметров интеграции с Kaspersky Security Center

Чтобы настроить параметры интеграции с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. С помощью переключателя в столбце **Статус** включите или выключите интеграцию с Kaspersky Security Center для тенанта.

   По умолчанию интеграция с Kaspersky Security Center для тенанта выключена.

4. Укажите интервалы для автоматического импорта информации об активах и уязвимостях активов из Kaspersky Security Center, выполнив следующие действия:

   a. Нажмите на имя тенанта в столбце **Тенант**.

   b. В открывшейся боковой панели в поле **KSC активы, информация об оборудовании** введите интервал в часах для автоматического импорта информации об основных атрибутах активов (состоянии защиты, версии антивирусных баз, оборудовании). Вы можете указать только целое число. Значение по умолчанию – `1` (1 час).

c. В поле **Атрибуты активов KSC (уязвимости, программное обеспечение, владельцы)** введите интервал в часах для автоматического импорта информации об остальных атрибутах активов (уязвимостях, программном обеспечении, владельцах). Вы можете указать только целое число. Значение по умолчанию – `12` (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.

При необходимости вы можете вручную импортировать информацию об активах и уязвимостях активов из Kaspersky Security Center.

5. Нажмите на кнопку **Сохранить**.

Параметры интеграции с Kaspersky Security Center для выбранного тенанта будут настроены.

Если в списке тенантов отсутствует требуемый тенант, вам нужно добавить тенант в список тенантов.

Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center

Чтобы добавить тенант в список тенантов для интеграции с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Нажмите на кнопку **Добавить параметры для нового тенанта**.

3. В открывшейся боковой панели **Kaspersky Security Center** в раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.

4. Нажмите на кнопку **Добавить**.

Выбранный тенант будет добавлен в список тенантов для интеграции с Kaspersky Security Center.

Удаление тенанта из списка тенантов для интеграции с Kaspersky Security Center

Чтобы удалить тенант из списка тенантов для интеграции с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. С помощью флажка выберите тенант, который хотите удалить.

3. Нажмите на кнопку **Удалить** и подтвердите удаление.

Выбранный тенант будет удален из списка тенантов для интеграции с Kaspersky Security Center.

Создание подключения к Kaspersky Security Center

Чтобы создать подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Нажмите на имя тенанта, для которого вы хотите создать подключение к Kaspersky Security Center.

3. В открывшейся боковой панели в блоке **Подключения** нажмите на кнопку **Создать** и укажите значения для следующих параметров:

   - **Статус** – статус подключения к выбранному серверу Kaspersky Security Center. Подключение может включаться и выключаться с помощью переключателя. По умолчанию подключение к выбранному серверу неактивно. В этом случае вы не можете использовать это подключение для соединения с сервером Kaspersky Security Center.

   - **Название** (обязательно) – имя подключения. Имя может включать от 1 до 128 символов в кодировке Unicode.

   - **URL** (обязательно) – URL сервера Kaspersky Security Center. Порт по умолчанию: 13299.

   - В раскрывающемся списке **Секрет** выберите секрет с учетными данными Kaspersky Security Center или **создайте новый секрет**.

     1. Нажмите на значок плюса (+).

        Откроется окно секрета.

     2. Введите данные секрета:

        a. В поле **Название** выберите имя для добавляемого секрета.

        b. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать учетные данные Kaspersky Security Center.

        c. В раскрывающемся списке **Тип** выберите **credentials**.

        d. В полях **Пользователь** и **Пароль** введите учетные данные вашего сервера Kaspersky Security Center.

        e. В поле **Описание** можно добавить описание секрета.

     3. Нажмите **Сохранить**.

     Выбранный секрет можно изменить, нажав на значок ✎.

4. Если вы хотите, чтобы решение KUMA импортировало только активы, которые подключены к подчиненным серверам или включены в группы, выполните следующие действия:

   a. Убедитесь, что подключение для соединения с сервером Kaspersky Security Center включено.

   b. В блоке **Иерархия** нажмите на кнопку **Загрузить**.

c. Выберите серверы и группы, из которых вы хотите импортировать информацию об активах.

d. Если вы хотите импортировать активы только из новых групп, установите флажок **Импортировать активы из новых групп**.

5. Если вы хотите, чтобы решение KUMA импортировало информацию об активах всех серверов Kaspersky Security Center, выполните следующие действия:

   a. Убедитесь, что подключение для соединения с сервером Kaspersky Security Center включено.

   b. Если вы хотите импортировать информацию об основных параметрах активов, нажмите на кнопку **Импортировать активы KSC**.

   c. Если вы хотите импортировать информацию об остальных параметрах активов, нажмите на кнопку **Импортировать атрибуты активов KSC**.

6. Нажмите на кнопку **Сохранить**.

Подключение к серверу Kaspersky Security Center будет создано. Его можно использовать для импорта информации об активах из Kaspersky Security Center в KUMA и для создания задач, связанных с активами, в Kaspersky Security Center из KUMA.

Изменение подключения к Kaspersky Security Center

Чтобы изменить подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Нажмите на имя тенанта, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Kaspersky Security Center**.

3. Нажмите на название подключения с Kaspersky Security Center, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к Kaspersky Security Center.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к Kaspersky Security Center будет изменено.

Удаление подключения к Kaspersky Security Center

Чтобы удалить подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Интеграции** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Нажмите на имя тенанта, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Kaspersky Security Center**.

3. Выберите подключение Kaspersky Security Center, которое вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

Подключение к Kaspersky Security Center будет удалено.

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, [OOTB] KSC MySQL или [OOTB] KSC PostgreSQL.
- 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 веб-интерфейсе KUMA в разделе **Ресурсы** в блоке **Ресурсы** выберите **Коннекторы**.

   b. Найдите в структуре папок нужный предустановленный коннектор, установите флажок рядом с этим коннектором и нажмите **Дублировать**.

   c. 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())
```

d. В блоке **Соединение** в раскрывающемся списке **Тип базы данных** выберите тип используемой базы данных.

e. При необходимости установите флажок **Секрет отдельно**. и укажите значение секрета в поле **Секрет**.

f. Установите курсор в поле **URL** и в раскрывшемся списке в строке используемого секрета нажмите на значок ✎.

g. 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 **Сохранить**.

h. В окне **Создание коннектора** в блоке **Соединение** 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 **Создать**.

2. Установите коллектор в веб-интерфейсе:

   a. Запустите мастер установки коллектора одним из следующих способов:

      - В веб-интерфейсе KUMA в разделе **Ресурсы** в блоке **Конфигурация сервисов** нажмите **Подключить источник**.

      - В веб-интерфейсе KUMA в разделе **Ресурсы** в блоке **Конфигурация сервисов** выберите **Коллекторы** и нажмите **Добавить**.

   b. На шаге 1 **Подключение источников** 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 **Сохранить и создать 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**.

https://rutube.ru/video/7e876600705999b2ce9f12602c76c9df/

Интеграция с Kaspersky Endpoint Detection and Response

Начиная с версии KATA 8.0 интеграция с Kaspersky Endpoint Detection and Response и импорт телеметрии Kaspersky Endpoint Detection and Response в KUMA не поддерживается. Реагирование через KEDR недоступно, запуск реагирования для активов завершаются ошибкой. Доступен только импорт событий действий платформы и событий алертов.

Kaspersky Endpoint Detection and Response (далее также KEDR) – функциональный блок приложения Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту активов локальной сети организации.

Вы можете настроить интеграцию KUMA с Kaspersky Endpoint Detection and Response 4.0 и выше, чтобы управлять действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response, и активах Kaspersky Security Center. Команды на выполнение операций поступают на сервер Kaspersky Endpoint Detection and Response, после чего она передает их программе Kaspersky Endpoint Agent, установленной на активах.

Для управления действиями по реагированию Kaspersky Endpoint Detection and Response на активах Kaspersky Security Center требуется, чтобы для актива в системе (поле Full device name) было указано полное доменное имя (FQDN). В противном случае запуск действий по реагированию недоступен.

Также вы можете импортировать события в KUMA и получать информацию об обнаружениях Kaspersky Endpoint Detection and Response (подробнее о получении информации об обнаружениях см. в разделе *Настройка интеграции с SIEM-системой* в справке Kaspersky Anti Targeted Attack Platform).

При интеграции KUMA с Kaspersky Endpoint Detection and Response вы можете выполнять следующие операции на активах Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent:

- Управлять сетевой изоляцией активов.
- Управлять правилами запрета.
- Запускать программы.

За инструкцией по настройке интеграции для управления действиями по реагированию вам требуется обратиться к вашему аккаунт-менеджеру или в службу технической поддержки.

Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kafka

При импорте событий из Kaspersky Endpoint Detection and Response телеметрия передается открытым текстом и может быть перехвачена злоумышленником.

Вы можете импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.0, 4.1, 5.0 и 5.1 с помощью коннектора Kafka.

При импорте событий из Kaspersky Endpoint Detection and Response 4.0 и 4.1 действует ряд ограничений:

- Импорт событий доступен, если в программе Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.
- Импорт событий **не** доступен, если в составе программы Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Для импорта событий вам потребуется выполнить действия на стороне Kaspersky Endpoint Detection and Response и на стороне KUMA.

Импорт событий Kaspersky Endpoint Detection and Response 4.0 или 4.1

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.0 или 4.1, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента программы.
3. В меню администратора компонента программы выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. Выполните команду:

   ```
   sudo -i
   ```
7. В конфигурационном файле `/etc/sysconfig/apt-services` в поле `KAFKA_PORTS` удалите значение `10000`.

   Если к серверу Central Node подключены серверы Secondary Central Node или компонент Sensor, установленный на отдельном сервере, вам требуется разрешить соединение с сервером, на котором вы изменили конфигурационный файл, по порту 10000.

   Мы не рекомендуем использовать этот порт для каких-либо внешних подключений, кроме KUMA. Чтобы ограничить подключение по порту 10000 только для KUMA, выполните команду:

```
iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
```

8. В конфигурационном файле `/usr/bin/apt-start-sedr-iptables` в поле `WEB_PORTS` добавьте значение `10000` через запятую без пробела.

9. Выполните команду:

```
sudo sh /usr/bin/apt-start-sedr-iptables
```

Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> centralnode` в один из следующих файлов:

   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.

   - `/etc/hosts` – для Linux.

2. В веб-интерфейсе KUMA создайте коннектор типа Kafka.

   При создании коннектора укажите следующие параметры:

   - В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.

   - В поле **Topic** укажите `EndpointEnrichedEventsTopic`.

   - В поле **Consumer group** укажите любое уникальное имя.

3. В веб-интерфейсе KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге. В качестве нормализатора для коллектора используйте [OOTB] KEDR telemetry.

При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Импорт событий Kaspersky Endpoint Detection and Response 5.0 и 5.1

При импорте событий из Kaspersky Endpoint Detection and Response 5.0 и 5.1 действует ряд ограничений:

- Импорт событий доступен только для неотказоустойчивой версии Kaspersky Endpoint Detection and Response.

- Импорт событий доступен, если в программе Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.

- Импорт событий **не** доступен, если в составе программы Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 5.0 или 5.1, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента программы.

3. В меню администратора компонента программы выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. В конфигурационном файле `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` укажите дополнительный порт `10000` для константы `WEB_PORTS`:

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

   Для версии Kaspersky Endpoint Detection and Response 5.1 этот шаг выполнять не нужно, порт указан по умолчанию.

7. Выполните команды:

   ```
   kata-firewall stop
   kata-firewall start --cluster-subnet <mask>
   ```

   где:

   <mask> – маска сети для адресации серверов кластера.

Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> kafka.services.external.dyn.kata` в один из следующих файлов:

   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.

   - `/etc/hosts` – для Linux.

2. В веб-интерфейсе KUMA создайте коннектор типа Kafka.

При создании коннектора укажите следующие параметры:

- В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.
- В поле **Topic** укажите `EndpointEnrichedEventsTopic`.
- В поле **Consumer group** укажите любое уникальное имя.

3. В веб-интерфейсе KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге. В качестве нормализатора для коллектора рекомендуется использовать нормализатор **[OOTB] KEDR telemetry**.

При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kata/edr

Чтобы импортировать события Kaspersky Endpoint Detection and Response версии 5.1 и старше с хостов с помощью коннектора kata/edr:

1. Выполните настройку на стороне KUMA для получения событий. Для этого создайте и установите в KUMA коллектор с коннектором kata/edr или внесите изменения в существующий коллектор, а затем сохраните измененные параметры и перезапустите коллектор.
2. На стороне KEDR примите запрос авторизации от KUMA, чтобы события начали поступать в KUMA.

В результате интеграция будет настроена, и события KEDR будут поступать в KUMA.

Создание коллектора для получения событий из KEDR

Чтобы создать коллектор для получения событий из KEDR:

1. В KUMA → **Ресурсы** → **Коллекторы** выберите **Добавить коллектор**.
2. В открывшемся окне **Создание коллектора** на шаге 1 **Подключение источников** укажите произвольное **Название коллектора** и выберите в раскрывающемся списке подходящий **Тенант**.
3. На шаге 2 **Транспорт** выполните следующие действия:
   1. На вкладке **Основные параметры**:
      a. В поле **Коннектор** выберите **Создать** или в этом же поле начните набирать название коннектора, если хотите использовать уже созданный коннектор.
      b. В раскрывающемся списке **Тип коннектора** выберите коннектор **kata/edr**. После того как вы выберите тип коннектора kata/edr, появятся дополнительные поля для заполнения.

c. В поле **URL** укажите адрес подключения к серверу KEDR в формате `<имя хоста или IP-адрес хоста>:<порт подключения, по умолчанию 443>`. Если решение KEDR развернуто в кластере, с помощью кнопки **Добавить** вы можете добавить все узлы. KUMA будет подключаться последовательно к каждому указанному узлу. Если решение KEDR установлено в распределенной конфигурации, на стороне KUMA необходимо настроить отдельный коллектор для каждого сервера KEDR.

d. В поле **Секрет** выберите **Создать**, чтобы создать новый секрет. В открывшемся окне **Создание секрета** укажите **Название** и нажмите **Сгенерировать и скачать сертификат и закрытый ключ шифрования соединения**.

   В результате в папку загрузок браузера, например Загрузки, будет скачан архив certificate.zip, который содержит файл ключа key.pem и файл сертификата cert.pem. Распакуйте архив. Нажмите **Загрузить сертификат** и выберите cert.pem. Нажмите **Загрузить закрытый ключ** и выберите key.pem. Нажмите **Создать**, после этого секрет будет добавлен в раскрывающийся список **Секрет** и будет автоматически выбран.

   Также вы можете выбрать из списка **Секрет** созданный секрет, с этим секретом KUMA будет подключаться к KEDR.

e. Поле **Внешний ID** содержит идентификатор для внешних систем. Этот идентификатор отображается в веб-интерфейсе KEDR при авторизации сервера KUMA. KUMA генерирует идентификатор автоматически и поле **Внешний ID** будет автоматически предзаполнено.

2. На вкладке **Дополнительные параметры**:

a. Чтобы получать детализированную информацию в журнале коллектора, переведите переключатель **Отладка** в активное положение.

b. При необходимости в поле **Кодировка символов** выберите кодировку исходных данных, к которым будет применена конвертация в UTF-8. Мы рекомендуем применять конвертацию только в том случае, если в полях нормализованного события отображаются недопустимые символы. По умолчанию значение не выбрано.

c. Укажите **Максимальное количество событий** в одном запросе к KEDR. По умолчанию указано значение 0 - это означает, что KUMA использует значение, заданное на сервере KEDR. Подробнее см. в Справке KATA. Вы можете указать произвольное значение, не превышающее значение на стороне KEDR. Если указанное вами значение превысит значение параметра **Максимальное количество событий**, заданное на сервере KEDR, в журнале коллектора KUMA будет ошибка *Bad Request: max_events N is greater than allowed value*.

d. Заполните поле **Время ожидания получения событий**, чтобы получать события через заданный промежуток времени. По умолчанию указано значение 0. Это означает, что применяется значение, заданное по умолчанию на сервере KEDR. Подробнее см. в Справке KATA. В этом поле указано время, по истечении которого сервер KEDR передаст KUMA события. На сервере KEDR действует два параметра: максимальное количество событий и время ожидания получения событий, передача событий происходит в зависимости от того, что произойдет раньше - будет собрано заданное количество событий или истечет заданное время. Если заданное время истекло, а заданного количества событий не набралось, сервер KEDR передаст те, что есть.

e. В поле **Время ожидания ответа** укажите максимальное значение ожидания ответа от сервера KEDR в секундах. Значение по умолчанию: 1800 сек, отображается как 0. В поле **Время ожидания ответа** указано клиентское ограничение. Значение параметра **Время ожидания ответа** должно быть больше, чем серверное **Время ожидания получения событий**, чтобы не прервать текущую задачу сбора событий новым запросом и дождаться ответа сервера. Если ответ от сервера KEDR все же не поступил, KUMA повторит запрос.

f. В поле **Фильтр KEDRQL** укажите условия фильтрации запроса. В результате со стороны KEDR будут поступать уже отфильтрованные события. Подробнее о доступных полях для фильтрации см. в Справке KATA.

4. На шаге 3 **Парсинг** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** выберите в раскрывающемся списке нормализатор [OOTB] KEDR telemetry.

5. Чтобы завершить создание коллектора в веб-интерфейсе, нажмите **Сохранить и создать сервис**. Затем скопируйте в веб-интерфейсе команду установки коллектора и выполните команду установки в интерпретаторе командной строки на сервере, где вы хотите установить коллектор.

   Если вы вносили изменения в существующий коллектор, нажмите **Сохранить и перезапустить сервисы**.

В результате коллектор создан и готов к отправке запросов, при этом коллектор будет отображаться в разделе **Ресурсы** → **Активные сервисы** в желтом статусе, пока на стороне KEDR не будет принят запрос авторизации от KUMA.

Авторизация KUMA на стороне KEDR

После того, как в KUMA создан коллектор, на стороне KEDR необходимо принять запрос авторизации KUMA, чтобы запросы от KUMA начали поступать в KEDR. После принятой авторизации коллектор KUMA автоматически по расписанию отправляет запрос в KEDR и ждет ответа. Все время ожидания статус коллектора будет желтый, а после получения первого ответа на отправленный запрос статус коллектора сменится на зеленый.

В результате интеграция настроена и вы можете просмотреть поступающие из KEDR события в разделе KUMA → **События**.

При первом запросе поступит часть исторических событий, которые произошли до момента интеграции. Когда все исторические события поступят, начнут поступать текущие события. Если вы измените значение параметра **URL** или **Внешний ID** для существующего коллектора, KEDR примет запрос как новый и после запуска коллектора KUMA с измененными параметрами вы снова получите часть исторических событий. Если вы не хотите получать исторические события, перейдите в параметры настройки нужного коллектора, настройте в нормализаторе сопоставление полей `timestamp` KEDR и KUMA и на шаге мастера установки коллектора Фильтрация событий укажите фильтр по `timestamp` так, чтобы значение `timestamp` событий было больше, чем значение `timestamp` запуска коллектора.

Возможные ошибки и способы решения

Если в журнале коллектора ошибка *Conflict: An external system with the following ip and certificate digest already exists. Either delete it or provide a new certificate*, необходимо создать новый секрет с новым сертификатом в коннекторе коллектора.

Если в журнале коллектора возникает ошибка *Continuation token not found* в ответ на запрос событий, нужно создать новый коннектор, прикрепить его к коллектору и перезапустить коллектор, или создать новый секрет с новым сертификатом в коннекторе коллектора. Если нет необходимости получать события, которые были сформированы до возникновения ошибки, следует настроить в коллекторе фильтр по Timestamp.

Настройка отображения ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации о событии KUMA

При получении обнаружений Kaspersky Endpoint Detection and Response в KUMA можно настроить создание алерта для каждого обнаружения. Вы можете настроить отображение ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации об алерте KUMA.

Вы можете настроить отображение ссылки на обнаружение, если используете только один сервер Central Node Kaspersky Endpoint Detection and Response. Если Kaspersky Endpoint Detection and Response используется в режиме распределенного решения, настроить отображение ссылок в KUMA на обнаружения Kaspersky Endpoint Detection and Response невозможно.

Для настройки отображения ссылки на обнаружение в информации об алерте KUMA вам требуется выполнить действия в веб-интерфейсе Kaspersky Endpoint Detection and Response и KUMA.

В веб-интерфейсе Kaspersky Endpoint Detection and Response вам нужно настроить интеграцию программы с KUMA в качестве SIEM-системы. Подробнее о том, как настроить интеграцию, см. в справке *Kaspersky Anti Targeted Attack Platform* в разделе *Настройка интеграции с SIEM-системой*.

Настройка отображения ссылки в веб-интерфейсе KUMA включает следующие этапы:

1. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории.

2. Создание правила корреляции.

3. Создание коррелятора.

4. Добавление коллектора, при котором следует учесть следующее:

   - На шаге **Транспорт** требуется указать тип коннектора (TCP или UDP) и порт подключения (значение должно совпадать со значением, установленным в параметрах подключения к SIEM в Kaspersky Anti Targeted Attack Platform).

   - На шаге **Парсинг** при выборе нормализатора требуется указать сопоставления для полей KEDR-событий или выбрать нормализатор `[OOTB] KATA`.

   - После добавления коррелятора требуется указать в коллекторе точку назначения в коррелятор.

Вы можете использовать преднастроенное корреляционное правило. В этом случае настройка отображения ссылки в веб-интерфейсе KUMA включает следующие этапы:

1. Создание коррелятора.

   В качестве правила корреляции вам нужно выбрать правило `[OOTB] KATA Alert`.

2. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории `KATA standAlone`.

Шаг 1. Добавление актива и назначение ему категории

Предварительно вам нужно создать категорию, которая будет назначена добавляемому активу.

Чтобы добавить категорию:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.

2. На вкладке **Все активы** разверните список категорий тенанта, выполнив одно из следующих действий:

   - В блоке **Все тенанты** нажмите на значок меню (•••) и выберите **Развернуть все**.

   - В дереве объектов **Все тенанты** нажмите на значок стрелки (▸) рядом с его названием.

3. Выберите требуемую категорию или подкатегорию и выполните одно из следующих действий:

4. Нажмите на значок добавления (+).

5. Нажмите на значок меню (⋮) и выберите **Добавить подкатегорию**.

   В правой части окна веб-интерфейса откроется боковая панель **Добавить категорию**.

6. Укажите параметры категории:

   a. В поле **Название** введите название категории.

   b. В раскрывающемся списке **Родительская категория** выберите категории в дереве категорий.

   c. Из раскрывающегося списка **Тенант** выберите тенанта, если он не указан автоматически.

   d. 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**.

        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 с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	=, ilike	
ОС	=, ilike	Оператор **ilike** 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.
Полное доменное имя	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Уровень критичности уязвимостей CVE на активе. Возможные значения параметра CVSS – от 0 до 10. Для уязвимостей из Kaspersky Security Center неприменимо.

Количество CVE	>, >=, =, <=, <	Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Для категоризации по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		И
		`CVSS >= 6.5`

ПО	=, ilike	Категоризация по ПО, установленному на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
Версия ПО	=, ilike, in	Категоризация по номеру версии (сборки) ПО, установленного на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
КИИ	in	Можно выбрать более одного значения.
Группа KSC	=, ilike	Категоризация по названию группы администрирования Kaspersky Security Center, в которую помещен актив.
Последнее обновление антивирусных баз	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.

Последнее обновление информации	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление защиты	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Время начала последней сессии	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Статус 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	=	

Последнее появление в сети	>=,<=	Для выполнения категоризации 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*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Рейтинг AI	>,>=,=,<=,<	Категоризация по рейтингам активов, присвоенным AI-сервисами.
Статус	=, in	Категоризация по предустановленным статусам актива, присвоенным AI-сервисами.
Настраиваемое поле актива	=, ilike	Категоризация по значениям настраиваемых полей 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 запуска категоризации 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 регулярно привязывать к категории активы, для которых антивирусные базы не обновлялись более 1 часа до запуска категоризации.

   - 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 регулярно привязывать к категории активы, информация о которых обновилась за сутки до запуска категоризации; или указать значение **now/w** с оператором **<=**, чтобы регулярно привязывать к категории 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**.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

e. При необходимости укажите значения для следующих параметров:

- Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.

  Указанный уровень важности присваивается корреляционным событиям и алертам, связанным с этим активом.

- В поле **Описание** добавьте описание категории.

7. Нажмите на кнопку **Сохранить**.

Чтобы добавить актив:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.

2. Нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.

3. Укажите следующие параметры актива:

   a. В поле **Название актива** введите название актива.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать актив.

   c. В поле **IP-адрес** укажите IP-адрес сервера Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения. При необходимости вы можете добавить еще один или несколько IP-адресов сервера.

d. При необходимости укажите значения для следующих полей:

- В поле **Полное доменное имя** укажите FQDN сервера Central Node Kaspersky Endpoint Detection and Response.
- В поле **MAC-адрес** укажите MAC-адрес сервера Central Node Kaspersky Endpoint Detection and Response.
- В поле **Владелец** укажите имя владельца актива.
- В поле **Категории** выберите категорию тенанта.
- В раскрывающемся списке **Категории КИИ** выберите категорию критической информационной инфраструктуры ресурса.

4. При необходимости в блоке **Программное обеспечение** укажите название и версию используемой операционной системы.
5. При необходимости в блоке **Информация об оборудовании** укажите следующие параметры используемого оборудования:
   - Название, количество ядер и частоту процессора в МГц. При необходимости с помощью кнопки **Добавить процессор** вы можете дополнительно указать один или несколько процессоров.
   - Количество свободных байт на диске и объем диска в байтах. При необходимости с помощью кнопки **Добавить диск** вы можете дополнительно указать один или несколько дисков для использования.
   - Название, производителя и версию драйвера сетевой карты. При необходимости с помощью кнопки **Добавить сетевую карту** вы можете дополнительно указать одну или несколько сетевых карт.
   - Частоту ОЗУ в МГц и общий объем ОЗУ в байтах.
6. Нажмите на кнопку **Сохранить**.

Шаг 2. Добавление правила корреляции

Вы можете создать правило корреляции или использовать готовое правило `[OOTB] KATA Alert`.

Чтобы добавить правило корреляции:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В блоке **Ресурсы** выберите **Правила корреляции** и нажмите на кнопку **Добавить**.
3. На вкладке **Общие** укажите следующие параметры:
   a. В поле **Название** укажите название правила.
   b. В раскрывающемся списке **Тенант** выберите интересующий вас тенант.
   c. В раскрывающемся списке **Тип** выберите **simple**.
   d. В раскрывающемся списке **Теги** выберите один или несколько тегов для идентификации правила.

e. В поле **Наследуемые поля** добавьте следующие поля: **DeviceProduct**, **DeviceAddress**, **EventOutcome**, **SourceAssetID**, **DeviceAssetID**.

f. При необходимости укажите значения для следующих полей:

- В поле **Частота срабатывания** 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.
- В раскрывающемся списке **Техники MITRE** выберите применимые техники MITRE ATT&CK.

4. На вкладке **Селекторы** → **Параметры** укажите следующие параметры фильтра:

a. В раскрывающемся списке **Фильтр** выберите **Создать**.

b. Нажмите на кнопку **Добавить группу**.

c. В поле с оператором для добавленной группы выберите **И**.

d. Добавьте условие для фильтрации по значению KATA:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите **Поля события**.
4. В поле **Поля события** выберите **DeviceProduct**.
5. В поле **Оператор** выберите =.
6. В поле **Правый операнд** выберите **Константа**.
7. В поле **значение** введите KATA.

e. Добавьте условие для фильтрации по категории:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите **Поля события**.
4. В поле **Поля события** выберите **DeviceAssetID**.
5. В поле **Оператор** выберите **inCategory**.
6. В поле **Правый операнд** выберите **Константа**.
7. Нажмите на кнопку **Конструктор**.

8. Выберите категорию, в которую вы поместили актив сервера Central Node Kaspersky Endpoint Detection and Response.

9. Нажмите на кнопку **Сохранить**.

f. В поле **Условия** нажмите на кнопку **Добавить группу**.

g. В поле с оператором для добавленной группы выберите **ИЛИ**.

h. Добавьте условие для фильтрации по идентификатору класса события:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.

2. В поле с условием выберите **Если**.

3. В поле **Левый операнд** выберите **Поля события**.

4. В поле **Поля события** выберите **DeviceEventClassID**.

5. В поле **Оператор** выберите =.

6. В поле **Правый операнд** выберите **Константа**.

7. В поле **Значение** введите **taaScanning**.

i. Повторите шаги 1–7 пункта h для каждого из следующих идентификаторов классов событий:

- file_web.
- file_mail.
- file_endpoint.
- file_external.
- ids.
- url_web.
- url_mail.
- dns.
- iocScanningEP.
- yaraScanningEP.

5. На вкладке **Действия** укажите следующие параметры:

a. Установите флажок **В дальнейшую обработку**.

b. В разделе **Обогащение** нажмите на кнопку **Добавить обогащение**.

c. В раскрывающемся списке **Исходный тип** выберите **Шаблон**.

d. В поле **Шаблон** введите `https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}`.

e. В раскрывающемся списке **Целевое поле** выберите **DeviceExternalID**.

> Для того чтобы параметр **DeviceExternalID** отображался в виде ссылки в свойствах событий, убедитесь, что в поле **Шаблон** для параметра `DeviceAddress` указаны URL или полное доменное имя, после которых присутствует символ "/", например: `https://example.com:8443/` или `https://example.com/`.

f. При необходимости переведите переключатель **Отладка** в активное положение, чтобы зарегистрировать информацию, связанную с работой ресурса, в журнал.

6. Нажмите на кнопку **Сохранить**.

Шаг 3. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

После завершения создания коррелятора в информации об алертах, созданных при получении обнаружений из Kaspersky Endpoint Detection and Response, будет отображаться ссылка на эти обнаружения. Ссылка отображается в информации о корреляционном событии (раздел **Связанные события**), в поле **DeviceExternalID**.

> Если вы хотите, чтобы в поле DeviceHostName в информации об обнаружении отображался FQDN сервера Central Node Kaspersky Endpoint Detection and Response, вам нужно создать запись для этого сервера в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

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 веб-интерфейсом CyberTrace доступна только для лицензии CyberTrace TIP Enterprise.

Также доступна настройка ретроспективного сканирования и обогащения событий через CyberTrace. Это позволяет KUMA получать оповещения по событиям, в которых индикаторы угроз не были обнаружены сразу, но стали известны позже после обновления потоков данных. Благодаря этому повышается точность выявления угроз на основе ранее зарегистрированных событий.

https://rutube.ru/video/3ffef45983cce034a42985364aab959f/

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 KUMA.

   В правиле обогащения вы можете указать, какими данными из CyberTrace вы хотите дополнить событие. В качестве типа источника данных рекомендуется выбрать cybertrace-http.

3. Создать коллектор для получения событий, которые вы хотите обогатить данными из CyberTrace.

4. Привязать правило обогащения к коллектору.

5. Сохранить и создать сервис:

   - 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 сервисы**, 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
Название	Test CT enrichment
Тенант	Общий
Тип источника данных	cybertrace-http
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 **Сохранить и создать сервис**.

   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 веб-интерфейс KUMA и нажмите **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
```

   Результат:

   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, мы рекомендуем:

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 программы.

Чтобы настроить CyberTrace для приема и обработки запросов в мастере первоначальной настройки:

1. Дождитесь запуска мастера первоначальной настройки CyberTrace после установки программы.

   Откроется шаг 1 **Добро пожаловать в Kaspersky CyberTrace**. Переход между шагами мастера осуществляется с помощью кнопки **Далее**.

2. На шаге 2 **Настройка прокси-сервера**, если в вашей организации используется прокси-сервер, укажите параметры соединения с ним. Если в вашей организации не используется прокси-сервер, оставьте все поля незаполненными.

3. На шаге 3 **Настройка лицензирования** выберите метод добавления лицензионного ключа для программы CyberTrace: с помощью кода активации или с помощью файла лицензионного ключа. В зависимости от выбранного метода укажите код активации или загрузите файл лицензионного ключа.

4. На шаге 4 **Настройка сервиса** оставьте значения по умолчанию.

5. На шаге 5 **Настройка управления данными** выполните следующие действия:

   a. В раскрывающемся списке **SIEM-система** выберите **KUMA**.

   b. В блоке параметров **Прослушивать** выберите вариант **IP-адрес и порт**.

   c. В поле **IP-адрес** укажите `0.0.0.0`.

   d. В поле **Порт** укажите порт для получения событий. Порт по умолчанию `9999`.

   e. В блоке параметров **Отправлять оповещения об обнаружении индикаторов компрометации** в поле **IP-адрес** укажите `127.0.0.1` и в поле **Порт** укажите `9998`.

   Остальные значения оставьте по умолчанию.

6. На шаге 6 **Настройка сертификата** выберите опцию **Коммерческий сертификат** и добавьте сертификат, позволяющий скачивать с серверов обновлений потоки данных (data feeds).

7. На шаге 7 **Настройка потоков данных** оставьте значения по умолчанию.

CyberTrace настроен.

Чтобы настроить CyberTrace для приема и обработки запросов в веб-интерфейсе программы:

1. В окне веб-интерфейса программы CyberTrace перейдите в режим **Управление данными**: в левом меню выберите пункт **Система**, а затем в появившемся меню выберите пункт **General**.

2. Выберите раздел **Настройка** → **Общие**.

3. В блоке параметров **Прослушивать** выполните следующие действия:

   a. Выберите вариант **IP-адрес и порт**.

   b. В поле **IP-адрес** введите `0.0.0.0`.

   c. В поле **Порт** укажите порт для приема событий. Порт по умолчанию `9999`.

4. Выберите раздел **Настройка** → **Служебные оповещения**.

5. В поле **Формат служебных оповещений** введите `%Date% alert=%Alert%%RecordContext%`.

6. В поле **Формат контекста записей** введите `|%ParamName%=%ParamValue%`.

7. Выберите раздел **Настройка** → **Оповещения об обнаружении индикаторов компрометации**.

8. В поле **Формат оповещения** введите `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.

9. На вкладке **Контекст** в поле **Поля контекста** введите `%ParamName%:%ParamValue%`.

10. Перейдите в режим **Управление системой**: в левом меню выберите пункт **General**, а затем в появившемся меню выберите пункт **Система**.

11. Выберите раздел **Настройка** → **Сервис**.

12. В блоке параметров **Веб-интерфейс** в поле **IP-адрес или имя хоста** введите `127.0.0.1`.

13. В верхней панели инструментов нажмите на кнопку **Перезапустить сервис**.

14. Перезапустите сервер CyberTrace.

    CyberTrace настроен.

Создание правил обогащения событий

Чтобы создать правила обогащения событий:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Правила обогащения**.

   Отобразится список доступных правил обогащения.

2. Нажмите на кнопку **Добавить**, чтобы создать новое правило.

3. В открывшемся окне укажите параметры правила обогащения:

   a. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип источника данных** выберите **cybertrace-http**.

   d. В поле **URL** укажите URL сервера CyberTrace, к которому вы хотите подключиться. Например, *example.domain.com:443*.

   e. В поле **Секрет** выберите или создайте секрет для подключения.

   f. В раскрывающемся списке **Ключевые поля** выберите поля событий, используемые для обогащения событий данными из CyberTrace.

   g. При необходимости в поле **Время ожидания** укажите максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

   h. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять KUMA в секунду. Значение по умолчанию: `1000`.

   i. В поле **Время ожидания** укажите время в секундах, в течение которого KUMA 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.

   j. В поле **Максимальное кол-во событий в очереди обогащения** укажите максимальное количество событий, сохраняемое в очереди для переотправки. По умолчанию установлено значение 1000000.

   k. С помощью переключателя **Основная версия Cybertrace** укажите версию CyberTrace. Доступные значения: < 5 и ≥ 5. При выборе версии ≥ 5.0 запросы будут выполняться в тенанте General в CyberTrace и будут использовать новую версию API, соответствующий версии CyberTrace 5.0 и выше, а также в CyberTrace появится возможность отображения данных статистики и ретроспективного анализа по запросам обогащения из KUMA, которые выполнены через http. При выборе значения <5 запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: <5.

   l. С помощью переключателя **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

   m. В раскрывающемся списке **Теги** выберите теги для правила обогащения событий.

   n. При необходимости в поле **Описание** добавьте до 4000 символов в кодировке Unicode.

   o. В блоке **Параметры фильтра** 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 ↗.

4. Нажмите **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 **Индикаторы**. Вся информация о найденном индикаторе будет отображаться на странице **Сведения об индикаторе**.

Интеграция интерфейса CyberTrace

Вы можете интегрировать веб-интерфейс CyberTrace в веб-интерфейс KUMA. Когда эта интеграция включена, в веб-интерфейсе KUMA появляется раздел **CyberTrace** с доступом к веб-интерфейсу CyberTrace. Вы можете настроить интеграцию в разделе **Интеграции** → **Kaspersky CyberTrace** веб-интерфейса KUMA.

Чтобы интегрировать веб-интерфейс CyberTrace в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить**, чтобы создать новый секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу CyberTrace.

   Откроется окно создания секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   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 в кодировке Unicode.

4. Нажмите **Создать**.

   Учетные данные сервера CyberTrace сохранены и могут использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейс KUMA **Параметры** → **Интеграции** → **Kaspersky CyberTrace**.

   Откроется окно с параметрами интеграции CyberTrace.

6. Измените необходимые параметры следующим образом:

   - **Состояние** – переведите переключатель в активное положение, если хотите включить интеграцию веб-интерфейса CyberTrace в веб-интерфейс KUMA.

   - **Адрес сервера** (обязательно) – введите адрес сервера CyberTrace.

   - **Порт** (обязательно) – введите порт сервера CyberTrace, порт для доступа к веб-интерфейсу по умолчанию 443.

   - **Секрет** – в раскрывающемся списке выберите ранее созданный секрет с типом **credentials**.

   - **Разрешить хосты** – в раскрывающемся списке выберите хосты, 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**.

7. Вы можете настроить доступ к веб-интерфейсу CyberTrace следующими способами:

   - Использовать hostname или IP при входе в веб-интерфейс KUMA.

     Для этого в разделе Разрешить хосты нажмите Добавить хост и в появившемся поле укажите IP или hostname устройства,

     на котором развернут веб-интерфейс KUMA.

   - Использовать FQDN при входе в веб-интерфейс KUMA.

     Если для работы в веб-интерфейсе решения вы используете браузер Mozilla Firefox, данные в разделе CyberTrace могут не отображаться. В таком случае настройте отображение данных (см. следующую инструкцию).

8. Нажмите **Сохранить**.

CyberTrace теперь интегрирован с KUMA: раздел **CyberTrace** отображается в веб-интерфейсе KUMA.

*Чтобы настроить отображение данных в разделе **CyberTrace** при использовании FQDN для входа в KUMA в Mozilla Firefox:*

1. Очистите кеш браузера.

2. В строке браузера введите FQDN веб-интерфейса KUMA с номером порта 7222: https://kuma.example.com:7222.

   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-адреса веб-интерфейса KUMA будет создано исключение.

5. В строке браузера введите URL-адрес веб-интерфейса KUMA с номером порта 7220.

6. Перейдите в раздел **CyberTrace**.

   Данные отобразятся в разделе.

Обновление списка запрещенных объектов CyberTrace (Internal TI)

Если веб-интерфейс CyberTrace интегрирован в веб-интерфейс KUMA, 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 в CyberTrace**.

   Откроется окно подтверждения.

3. Если вы хотите подтвердить свои действия и обновить **Internal TI** данными из событий KUMA, нажмите **Да**.

   Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

Настройка обогащения событий и ретроспективного сканирования

Интеграция KUMA с Kaspersky CyberTrace (далее CyberTrace) версии 5.0 и выше позволяет обогащать события информацией об индикаторах компрометации (IoC) и выполнять ретроспективное сканирование событий. Ретроспективное сканирование помогает выявить индикаторы, которые не были обнаружены в момент первичного обогащения, но появились позднее в обновленных потоках данных CyberTrace. Ретроспективное сканирование может использоваться в следующих случаях:

- Инцидент уже произошел, но его признаки стали известны только после обновления потоков данных.
- Вы хотите перепроверить сохраненные события на наличие новых угроз.

Чтобы настроить обогащение данных и ретроспективное сканирование:

1. Выполните первоначальную настройку в KUMA, выполнив следующие шаги:

   a. Настройте интеграцию с CyberTrace.

   b. Создайте два коллектора для получения событий, которые вы хотите обогатить данными из CyberTrace:

      - Для приема оповещений о срабатывании индикаторов от CyberTrace создайте коллектор, в котором в качестве транспорта используется коннектор с типом **tcp**, а в качестве нормализатора используется **[OOTB] CyberTrace**.

      - Для настройки обогащения событий создайте коллектор со следующими параметрами:

        - В качестве транспорта выберите любой коннектор (например, **http**).

        - В качестве метода нормализации выберите любой метод (например, **json**) с сопоставлением следующих полей: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.

        - В качестве обогащения создайте правило обогащения событий, в котором тип источника данных – **cybertrace-http**, указана версия CyberTrace **≥ 5.0**, и в раскрывающемся списке **Ключевые поля** выбраны следующие поля нормализатора: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.

2. Выполните настройку ретроспективного сканирования в веб-интерфейсе CyberTrace, выполнив следующие шаги:

   a. В разделе **Настройка** → **Общие** включите **API lookup**, чтобы сохранять обнаруженные индикаторы и собирать по ним статистику при использовании запроса к публичному API.

   b. В разделе **Настройка** → **Ретроскан** включите ретроспективное сканирование, а затем откройте вкладку **Регулярные выражения** и включите те источники и их регулярные выражения, которые требуется использовать для ретроспективного сканирования.

   c. В разделе **Настройка** → **Общие** в блоке параметров **Оповещения об обнаружении индикаторов компрометации** укажите IP-адрес и порт, которые будут использоваться в CyberTrace для отправки оповещений об обнаружении индикаторов компрометации.

   d. В разделе **Настройка** → **Общие** в блоке параметров **Служебные оповещения** настройте отправку служебных оповещений CyberTrace (например, об окончании выполнения задачи ретроспективного сканирования или замене лицензионного ключа), указав IP-адрес коллектора и порт TCP-коннектора KUMA.

   Подробнее о настройке ретроспективного сканирования см. *справку Kaspersky CyberTrace*.

Этапы обработки событий в процессе ретроспективного сканирования

Ретроспективное сканирование позволяет выявлять индикаторы компрометации, которые не были известны на момент получения события, но стали доступны позже после обновления потоков данных Kaspersky CyberTrace.

Алгоритм работы ретроспективного сканирования состоит из следующих этапов:

1. **Отправка события в CyberTrace**

   В коллектор CyberTrace, настроенный на прием событий для обогащения, поступает событие, содержащее индикаторы. Эти индикаторы на момент получения могут отсутствовать в активных потоках данных.

   Пример события:

   ```
   {
   "SourceHostName": "45.54.64.52",
   "DestinationHostName": "geardox.site",
   "Message": "5BA7335AD847E5ED6211FB27094B9855",
   "DeviceHostName": "test.domain.ru",
   "DeviceAddress": "5.8.16.77",
   "FileHash": "E1B85D995DC09DE25603D0B7A67D998015F6C045",
   "OldFileHash": "B276263D373A6B56EEAB09673429E1490AEFC5E14738CDF9E1661C36EBD80656",
   "RequestUrl": "https://kaspersky.com/"
   }
   ```

2. **Сохранение события в базе данных CyberTrace**

   Если используется интеграция по TCP, CyberTrace извлекает индикаторы из события с помощью регулярных выражений. При интеграции через REST API (с использованием API lookup) индикаторы передаются непосредственно в теле запроса. Если на момент обработки индикатора в потоках данных отсутствует информация, позволяющая его классифицировать, CyberTrace сохраняет индикатор в базу данных ретроспективного сканирования для последующего анализа при обновлении потоков данных.

3. **Запуск задачи ретроспективного сканирования**

   Задача ретроспективного сканирования может запускаться по расписанию или вручную. Чтобы запустить ретроспективное сканирование вручную, перейдите на страницу **Система** → **Ретроскан** и нажмите **Начать сейчас**.

4. **Обнаружение индикаторов при обновлении потоков данных**

   Если в процессе обновления в потоках данных появились индикаторы, совпадающие с ранее сохраненными событиями, CyberTrace при выполнении задачи ретроспективного сканирования обнаружит такие совпадения.

5. **Формирование алертов по результатам ретроспективного сканирования**

   После завершения ретроспективного сканирования CyberTrace формирует оповещения об обнаружении индикаторов компрометации и направляет их в коллектор KUMA.

   Пример оповещения:

   ```
   Category=KUMA_Demo_1_Hash_SHA1|MatchedIndicator=E1B85D995DC09DE25603D0B7A67D998015F6C045|MD
   05:34|geo=bd, eg, in|last_seen=02.02.2021
   11:36|popularity=2|threat=HEUR:Trojan.MSIL.Taskun.gen
   ```

6. **Обработка события в KUMA**

   Событие обрабатывается нормализатором **[OOTB] CyberTrace**. Пользователь может сопоставить полученное оповещение с исходным событием для последующего анализа.

7. **Получение служебного оповещения о завершении задачи**

Если в CyberTrace настроена отправка служебных оповещений, CyberTrace отправит уведомление о завершении задачи ретроспективного сканирования.

Пример оповещения:

```
Jun 05 16:08:33
alert=KL_ALERT_RetroScanCompleted|iocs_detected=168|iocs_rescanned=1511177|retroscan_report
C2DF-4AED-B430-2E64AEF781FC
```

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 KUMA портал помогает пользователям KUMA быстрее принимать обоснованные решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, включая данные WHOIS и DNS.

В справке Kaspersky Threat Intelligence Portal вы можете найти информацию о предоставлении данных для следующих объектов:

- Хешах.
- IP-адресах.
- Доменах.
- Веб-адресах.

Доступ к Kaspersky Threat Intelligence Portal предоставляется на платной основе. Лицензионные сертификаты создаются специалистами "Лаборатории Касперского". Чтобы получить сертификат для Kaspersky Threat Intelligence Portal, обратитесь к вашему персональному техническому менеджеру "Лаборатории Касперского".

Инициализация интеграции с Kaspersky Threat Intelligence Portal

Чтобы интегрировать Kaspersky Threat Intelligence Portal в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы**.
2. В блоке **Ресурсы** выберите **Секреты**.

   Отобразится список доступных секретов.
3. Нажмите на кнопку **Добавить**, чтобы создать новый секрет. Этот ресурс используется для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.

   Откроется окно секрета.

4. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **ktl**.

   d. В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal.

5. Загрузите ключ сертификата Kaspersky Threat Intelligence Portal:

   a. Нажмите **Загрузить PFX** и выберите PFX-файл с сертификатом.

      Имя выбранного файла отображается справа от кнопки **Загрузить PFX**.

   b. В поле **Пароль PFX** введите пароль для PFX-файла.

6. При необходимости в раскрывающемся списке **Теги** выберите один или несколько тегов для секрета.

7. В поле **Описание** можно добавить описание секрета.

8. Нажмите **Создать**.

   Ваши учетные данные Kaspersky Threat Intelligence Portal сохранены и могут использоваться в других ресурсах KUMA.

9. Перейдите в раздел **Параметры** → **Интеграции** → **Интеграция с Kaspersky Threat Lookup**.

10. С помощью переключателя **Состояние** включите интеграцию. По умолчанию интеграция выключена.

11. В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.

    Можно создать новый секрет, нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы** → **Секреты**.

12. При необходимости в раскрывающемся списке **Прокси-сервер** выберите прокси-сервер.

13. Если вы хотите принять Соглашение о лицензии для получения данных OSINT, нажмите на ссылку **Соглашение о лицензии**. В появившемся окне **Соглашение о лицензии** выберите **Я принимаю соглашение** и нажмите **Сохранить**. Данные OSINT будут поступать в KUMA после того, как вы отправите запрос на обогащение данных от Kaspersky Threat Intelligence Portal, установив флажок **Данные OSINT** в параметрах обогащения.

14. Нажмите **Сохранить**.

15. После того, как вы сохраните настройки, выполните вход в веб-интерфейс и примите **Условия использования**, иначе в API будет возвращаться ошибка.

Процесс интеграции Kaspersky Threat Intelligence Portal с KUMA завершен.

После интеграции Kaspersky Threat Intelligence Portal и KUMA в области деталей события можно запрашивать сведения о хостах, доменах, URL-адресах, IP-адресах и хешах файлов (MD5, SHA1, SHA256).

Запрос данных от Kaspersky Threat Intelligence Portal

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

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.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

2. Установите флажки рядом с типами данных, которые нужно запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

3. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.

4. Нажмите **Запрос**.

Задача *ktl* создана. По ее завершении события дополняются данными из Kaspersky Threat Intelligence Portal, которые можно просмотреть в таблице событий, окне алерта или окне корреляционного события.

Просмотр данных от Kaspersky Threat Intelligence Portal

Чтобы просмотреть данные из Kaspersky Threat Intelligence Portal,

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, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.

Информация, полученная от Kaspersky Threat Intelligence Portal, кешируется. Если нажать на домен, веб-адрес, IP-адрес или хеш файла в области деталей события, для которого у KUMA уже есть доступная информация, вместо окна **Обогащение Threat Lookup** отобразятся данные из Kaspersky Threat Intelligence Portal с указанием времени их получения. Эти данные можно обновить.

Обновление данных от Kaspersky Threat Intelligence Portal

Чтобы обновить данные, полученные от Kaspersky Threat Intelligence Portal:

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, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

2. Нажмите **Обновить** в области деталей события с данными, полученными с портала Kaspersky Threat Intelligence Portal.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

3. Установите флажки рядом с типами данных, которые вы хотите запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

4. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.

5. Нажмите **Обновить**.

   Создается задача *KTL* и запрашиваются новые данные, полученные из Kaspersky Threat Intelligence Portal.

6. Закройте окно **Обогащение Threat Lookup** и область подробной информации о KTL.

7. Откройте область подробной информации о событии из таблицы событий, окна алертов или окна корреляционных событий и перейдите по ссылке, соответствующей домену, веб-адресу, IP-адресу или хешу файла, для которого вы обновили информацию на Kaspersky Threat Intelligence Portal, и выберите **Показать информацию из Threat Lookup**.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени.

Интеграция с R-Vision Security Orchestration, Automation and Response

R-Vision Security Orchestration, Automation and Response (далее R-Vision SOAR) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

R-Vision SOAR можно интегрировать с KUMA. Когда интеграция включена, создание алерта в KUMA приводит к созданию инцидента в R-Vision SOAR. Алерт KUMA и инцидент R-Vision SOAR взаимосвязаны: при обновлении статуса инцидента в R-Vision SOAR статус соответствующего алерта KUMA также меняется.

Интеграция R-Vision SOAR и KUMA настраивается в обоих решениях. На стороне KUMA настройка интеграции доступна только для главных администраторов.

Сопоставление полей алерта KUMA и инцидента R-Vision SOAR при передаче данных по API

Поле алерта KUMA	Поле инцидента R-Vision SOAR
`firstSeen`	`detection`
`priority`	`level`
`correlationRuleName`	`description`
`events` В виде json-файла)	`files`

Настройка интеграции в KUMA

В этом разделе описывается интеграция KUMA с R-Vision SOAR на стороне KUMA.

Интеграция в KUMA настраивается в разделе веб-интерфейса KUMA **Параметры** → **Интеграции** → **IRP / SOAR**.

Чтобы настроить интеграцию с R-Vision SOAR:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** и в блоке **Ресурсы** выберите **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить**, чтобы создать новый секрет. Этот ресурс будет использоваться для хранения токена для API-запросов в R-Vision SOAR.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** укажите имя для добавляемого секрета. Длина названия должна быть от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **token**.

   d. В поле **Токен** введите свой API-токен для R-Vision SOAR.

      Токен можно узнать в веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Общие** → **API**.

   e. При необходимости в раскрывающемся списке **Теги** выберите теги для секрета.

   f. При необходимости в поле **Описание** добавьте описание секрета до 4000 символов в кодировке Unicode.

4. Нажмите **Создать**.

   API-токен для R-Vision SOAR сохранен и теперь может использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейса KUMA **Параметры** → **Интеграции** → **IRP / SOAR**.

   Откроется окно с параметрами интеграции R-Vision SOAR.

6. С помощью переключателя **Состояние** включите интеграцию R-Vision SOAR с KUMA. По умолчанию интеграция выключена.

7. В раскрывающемся списке **Секрет** выберите секрет, созданный ранее.

   Можно создать новый секрет, выбрав **Создать**. Созданный секрет будет сохранен в разделе **Ресурсы** → **Ресурсы** → **Секреты**.

8. В поле **URL** укажите URL хоста сервера R-Vision SOAR.

9. В поле **Название поля для размещения идентификаторов алертов KUMA** укажите название поля R-Vision SOAR, в которое будет записываться идентификатор алерта KUMA.

10. В поле **Название поля для размещения URL алертов KUMA** укажите название поля R-Vision SOAR, в которое будет помещаться ссылка на алерт KUMA.

11. В поле **Категория** укажите категорию алерта R-Vision SOAR, который создается при получении данных об алерте от KUMA.

12. В раскрывающемся списке **Поля событий KUMA для отправки в IRP / SOAR** выберите поля событий KUMA, которые следует отправлять в R-Vision SOAR.

13. В блоке **Уровень важности** укажите значения уровней для сопоставления значений уровня важности KUMA со значениями уровня важности R-Vision SOAR.

14. Нажмите **Сохранить**.

    В KUMA теперь настроена интеграция с R-Vision SOAR. Если интеграция также настроена в R-Vision SOAR, при появлении алертов в KUMA информация о них будет отправляться в R-Vision SOAR для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision SOAR.

Если вы работаете с несколькими тенантами и хотите интегрироваться с R-Vision SOAR, названия тенантов должны соответствовать коротким названиям компаний в R-Vision SOAR.

Настройка интеграции в R-Vision SOAR

В этом разделе описывается интеграция KUMA с R-Vision SOAR на стороне R-Vision SOAR.

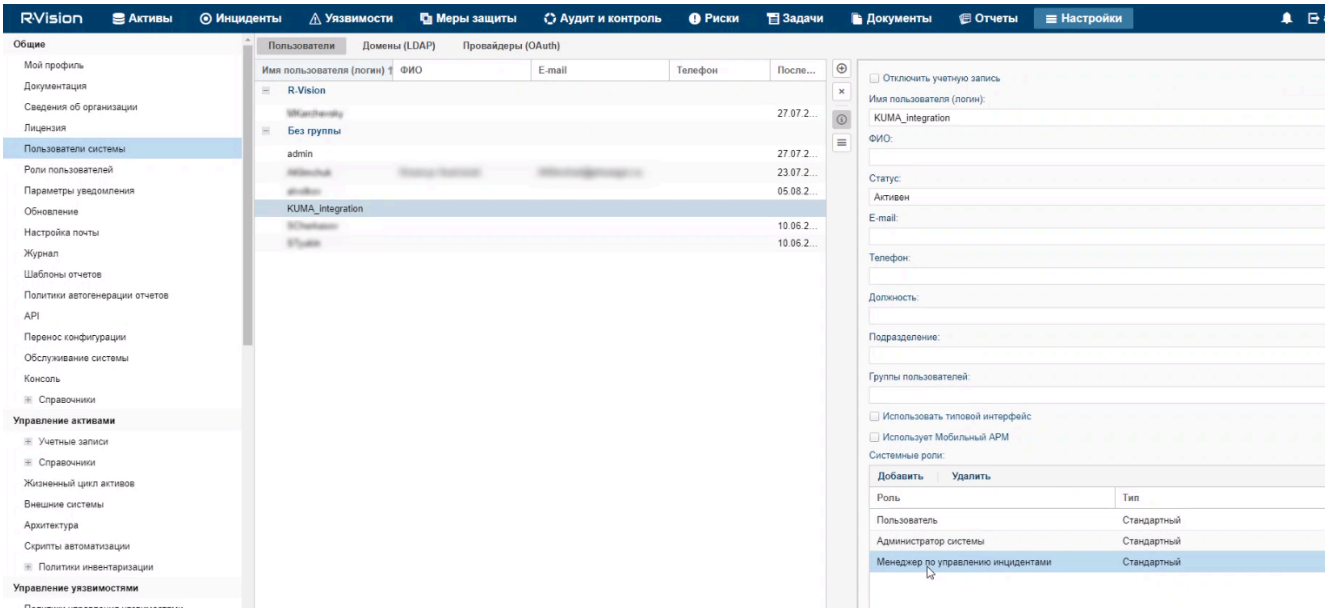
Интеграция в R-Vision SOAR настраивается в разделе **Настройки** веб-интерфейса R-Vision SOAR. Подробнее о настройке R-Vision SOAR см. в документации этой программы.

Настройка интеграции с KUMA состоит из следующих этапов:

- **Настройка роли пользователя R-Vision SOAR**

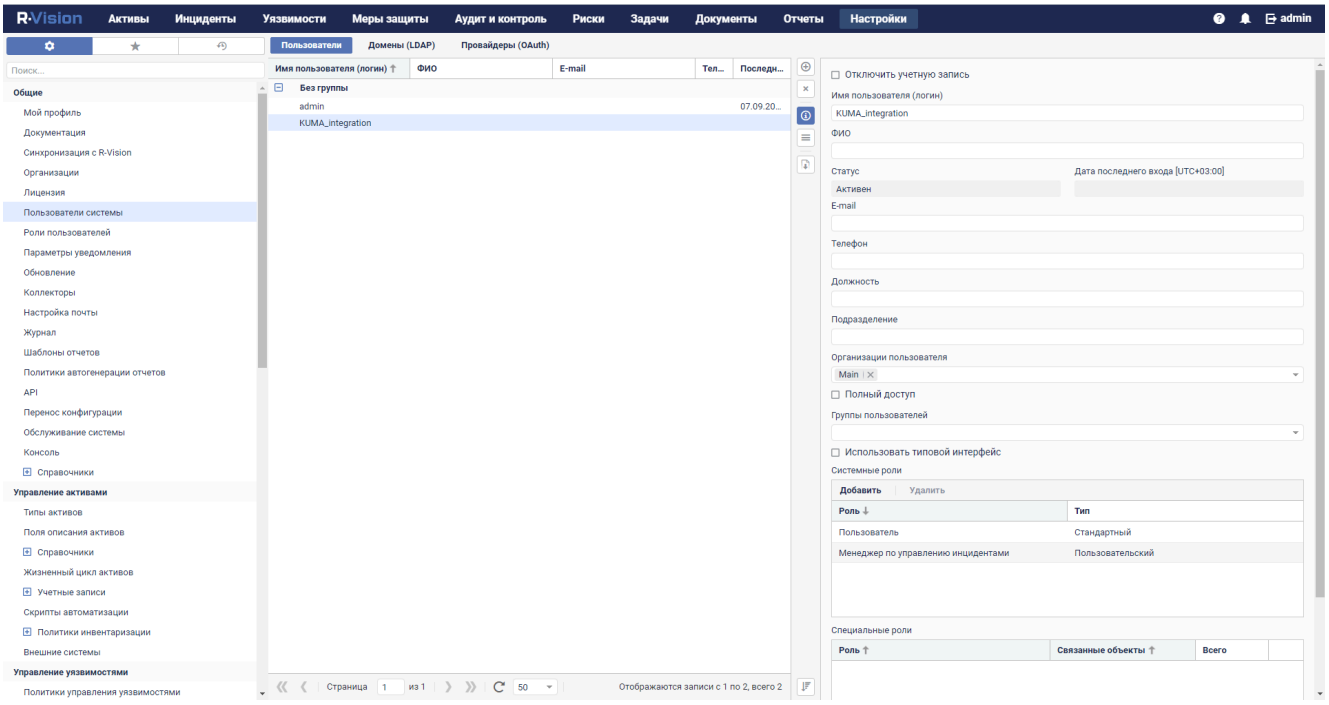
  1. Присвойте используемому для интеграции пользователю R-Vision SOAR системную роль **Менеджер по управлению инцидентами**. Роль можно присвоить в веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Общие** → **Пользователи системы**, выбрав нужного пользователя. Роль добавляется в блоке параметров **Системные роли** (см. рисунки по ссылкам ниже).

     Пользователь R-Vision SOAR версии 4.0 с ролью Менеджер по управлению инцидентами



Присвоение пользователю роли в R-Vision SOAR версии 4.0

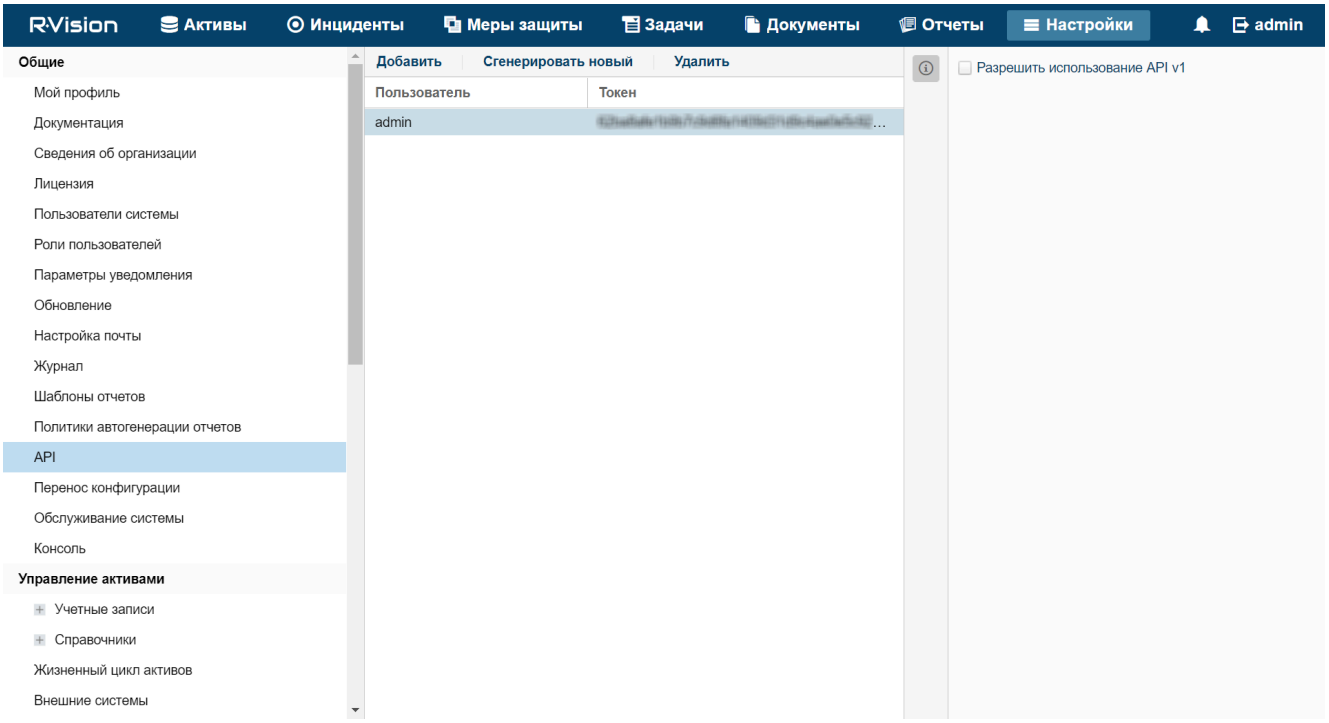
Пользователь R-Vision SOAR версии 5.0 с ролью Менеджер по управлению инцидентами



Присвоение пользователю роли в R-Vision SOAR версии 5.0

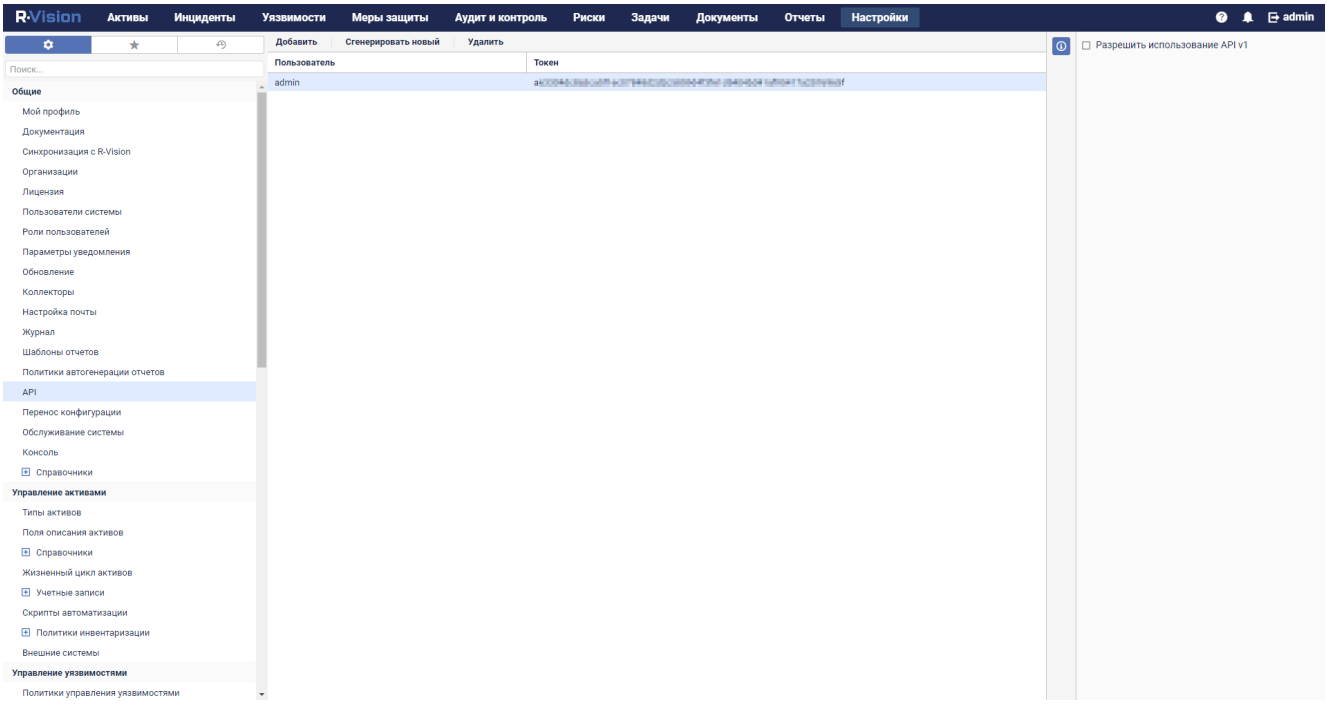
2. Убедитесь, что API-токен используемого для интеграции пользователя R-Vision SOAR указан в секрете в веб-интерфейсе KUMA. Токен отображается в веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Общие** → **API** (см. рисунки по ссылкам ниже).

API-токен в R-Vision SOAR версии 4.0



API-токен в R-Vision SOAR версии 4.0

API-токен в R-Vision SOAR версии 5.0



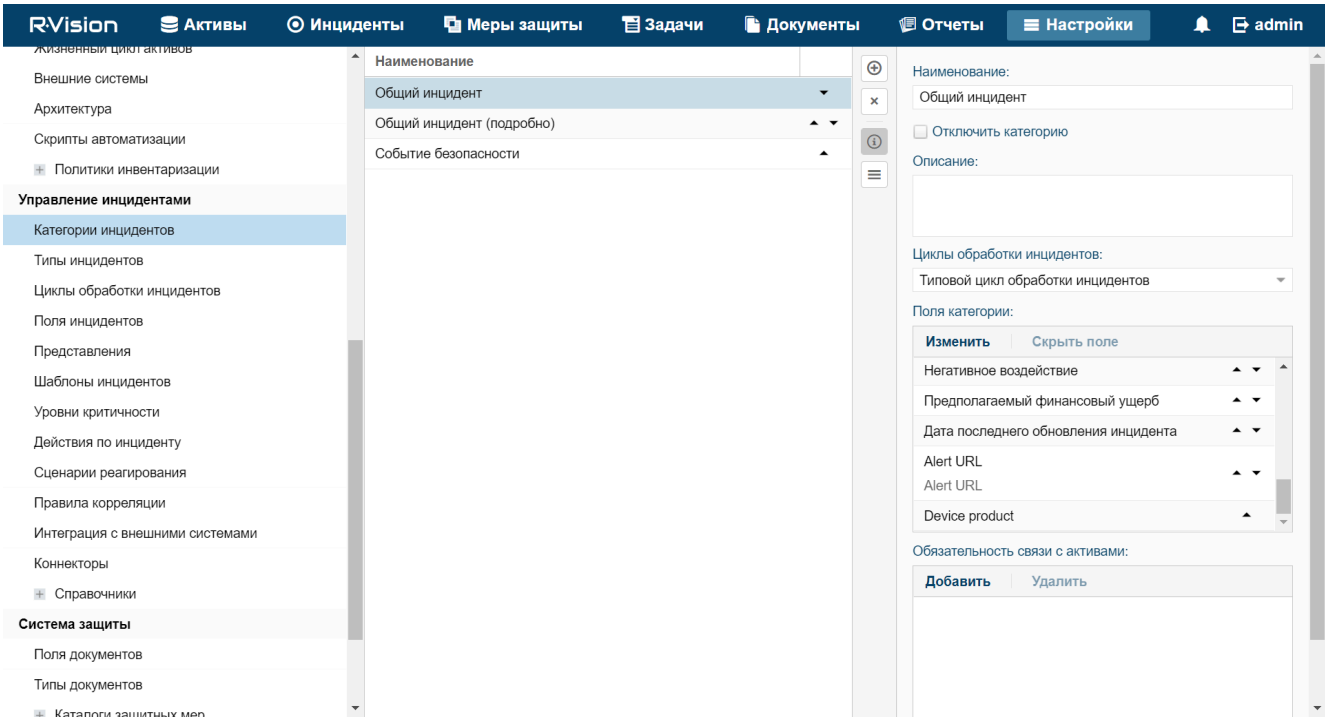
API-токен в R-Vision SOAR версии 5.0

- **Настройка полей инцидентов R-Vision SOAR и алертов KUMA**

  1. Добавьте поля инцидента ALERT_ID и ALERT_URL.

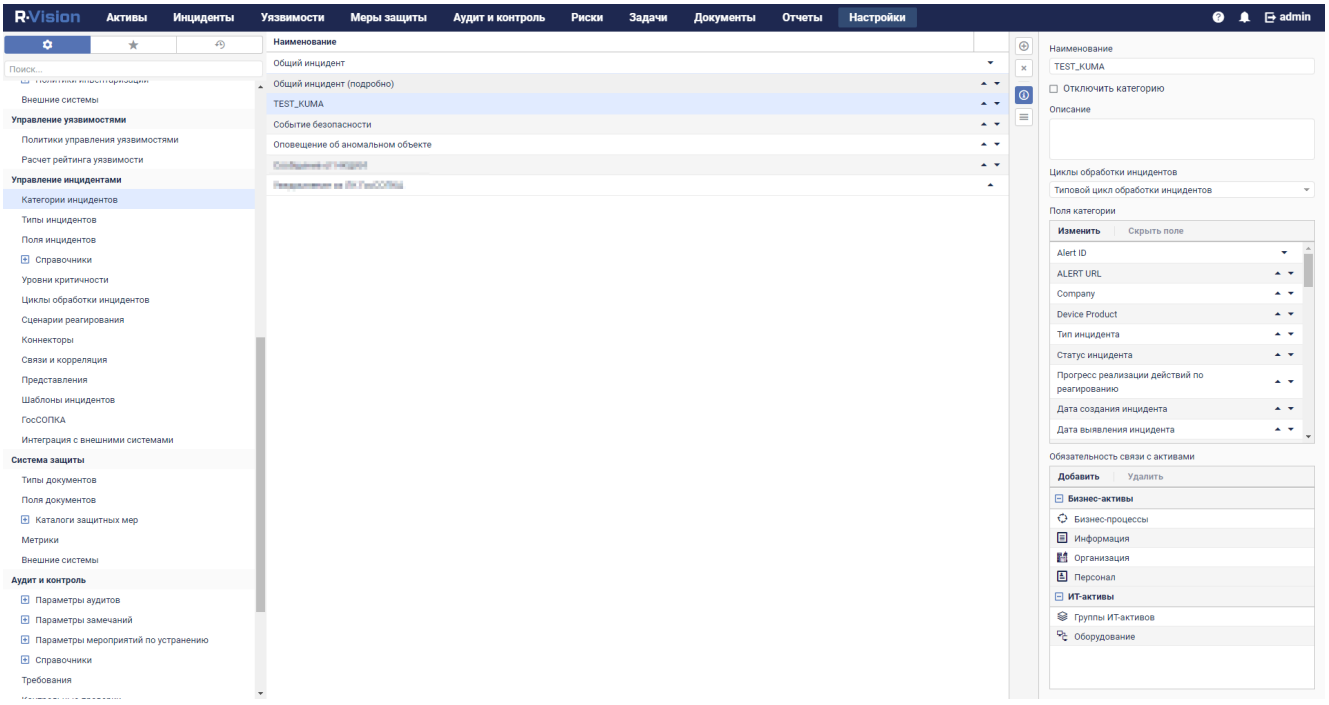
  2. Настройте категорию инцидентов R-Vision SOAR, создаваемых по алертам KUMA. Это можно сделать в веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Категории инцидентов**. Добавьте новую или измените существующую категорию инцидентов, указав в блоке параметров **Поля категорий** созданные ранее поля инцидентов `Alert ID` и `Alert URL` (см. рисунки по ссылкам ниже). Поле `Alert ID` можно сделать скрытым.

     Категории инцидентов с данными из алертов KUMA в R-Vision SOAR версии 4.0



Настройка полей в инцидентах R-Vision SOAR версии 4.0

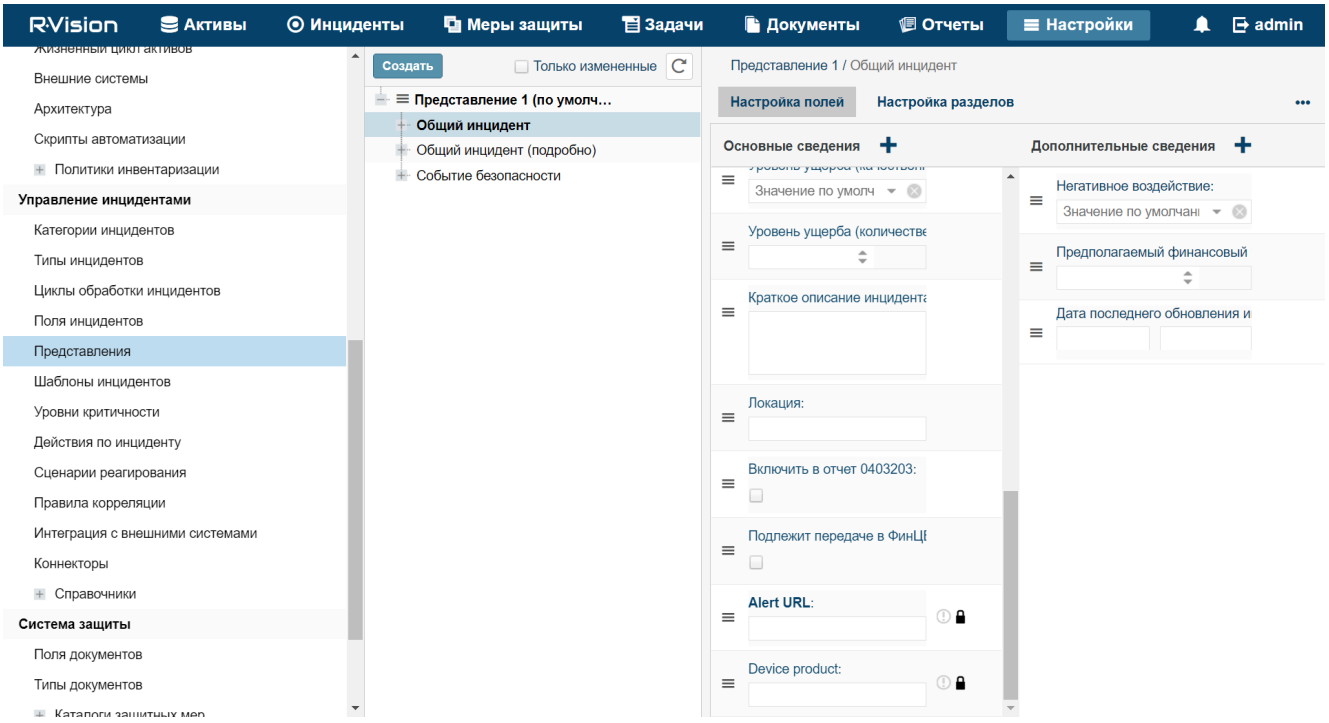
Категории инцидентов с данными из алертов KUMA в R-Vision SOAR версии 5.0



Настройка полей в инцидентах R-Vision SOAR версии 5.0

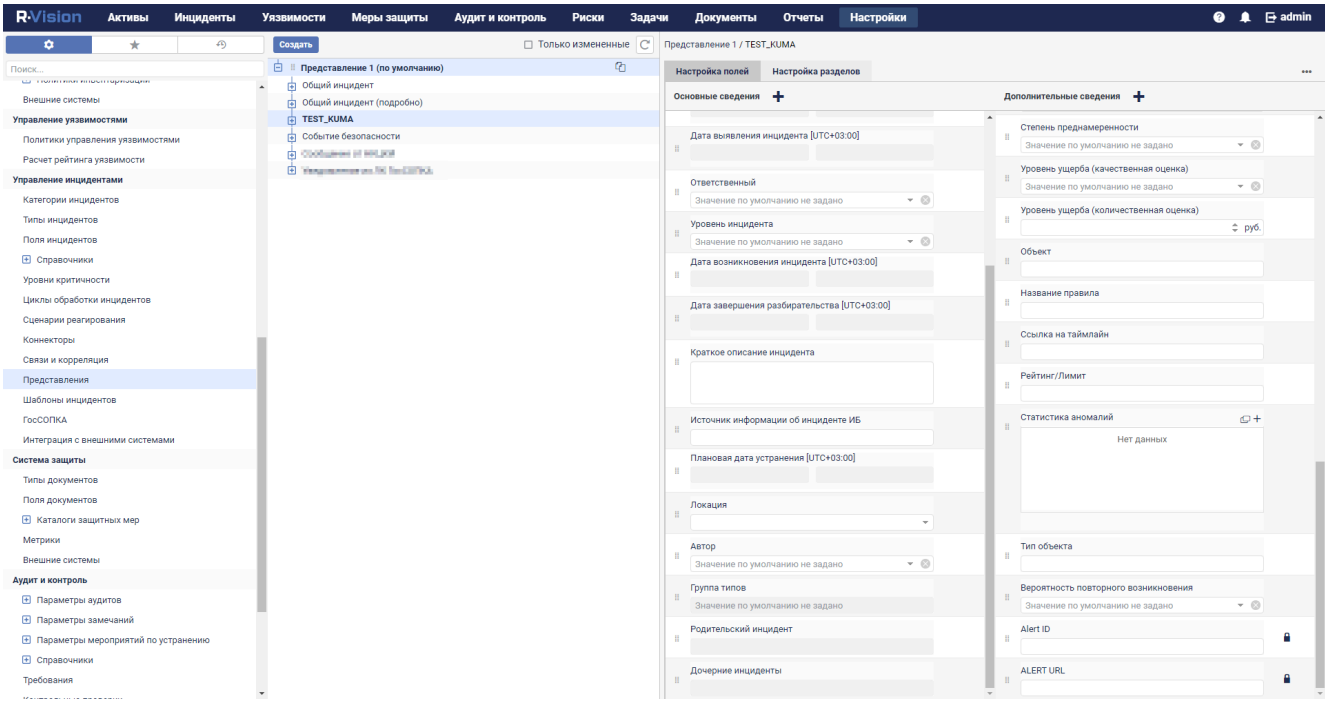
3. Запретите редактирование ранее созданных полей инцидентов `Alert ID` и `Alert URL`. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Представления** выберите категорию инцидентов R-Vision SOAR, которые будут создаваться по алертам KUMA, и установите рядом с полями `Alert ID` и `Alert URL` значок замка (см. рисунки по ссылкам ниже).

Поле Alert URL недоступно для редактирования в R-Vision SOAR версии 4.0



Установка запрета на редактирование полей в R-Vision SOAR версии 4.0

Поле Alert URL недоступно для редактирования в R-Vision SOAR версии 5.0



Установка запрета на редактирование полей в R-Vision SOAR версии 5.0

- **Создание коллектора и коннектора в R-Vision SOAR**

  1. Создайте коллектор R-Vision SOAR для взаимодействия с KUMA.

  2. Создайте и настройте коннектор R-Vision SOAR для отправки в KUMA API-запросов на закрытие алертов.

- **Создание правила на закрытие алерта в KUMA**

  Создайте правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision SOAR.

В R-Vision SOAR теперь настроена интеграция с KUMA. Если интеграция также настроена в KUMA, при появлении алертов в KUMA информация о них будет отправляться в R-Vision SOAR для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision SOAR.

Добавление полей инцидента ALERT_ID и ALERT_URL

Чтобы добавить в R-Vision SOAR поле инцидента ALERT_ID:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.

2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.

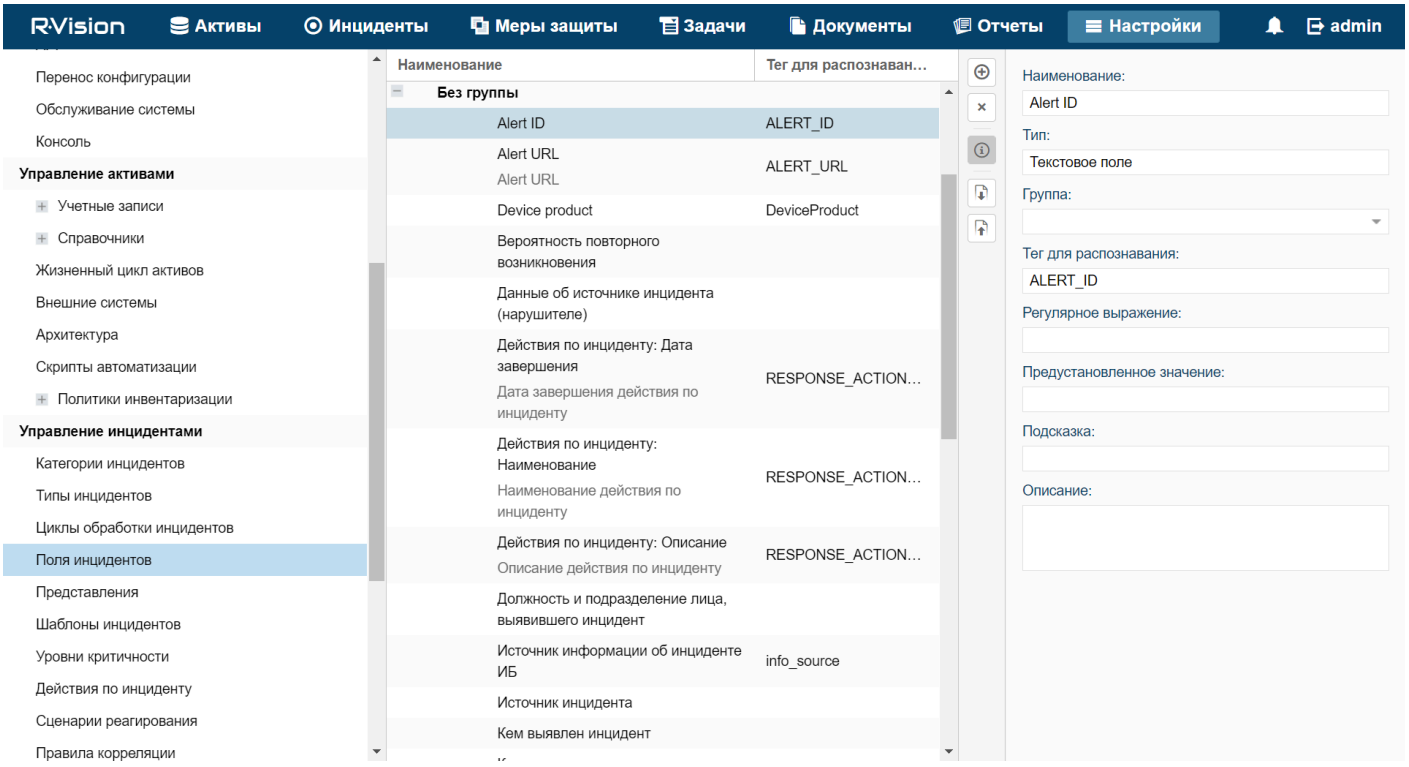
3. В поле **Наименование** введите название поля, например `Alert ID`.

4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.

5. В поле **Тег для распознавания** введите `ALERT_ID`.

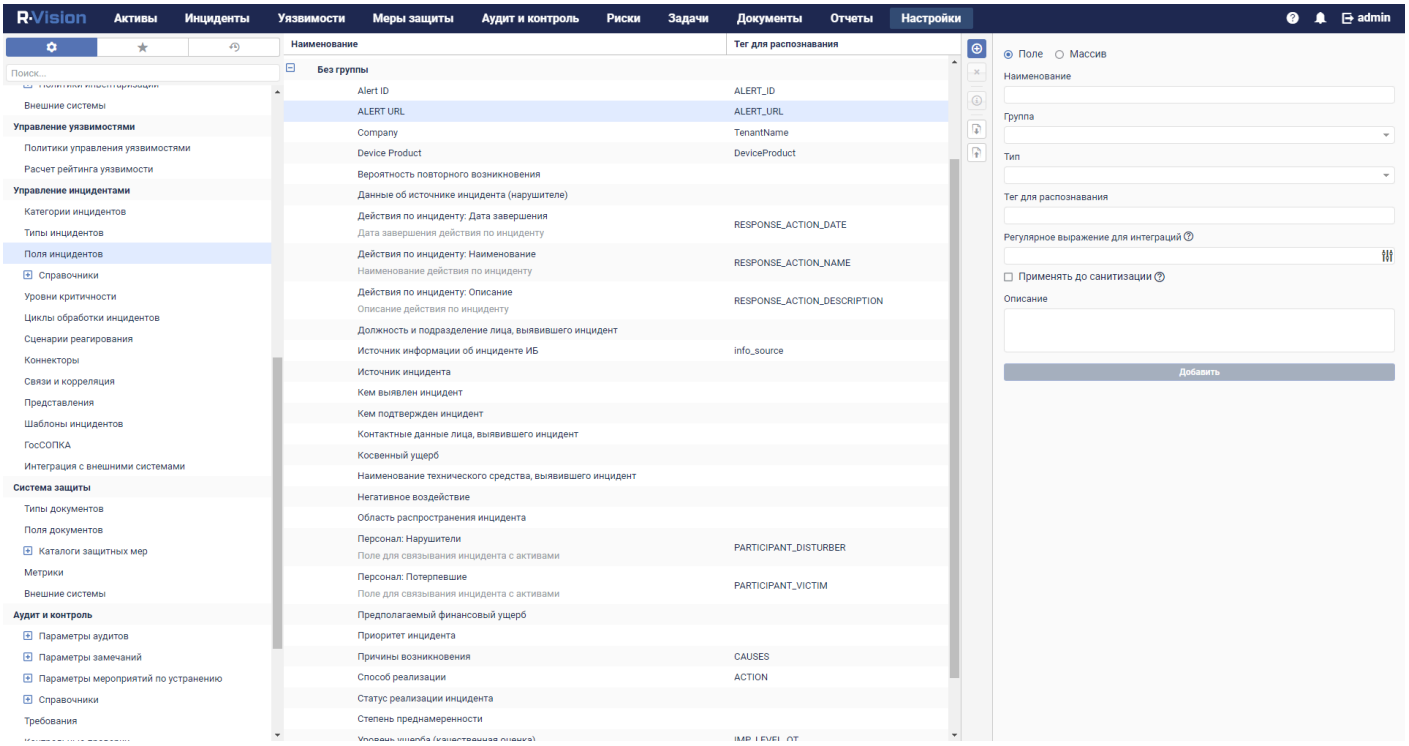
Поле ALERT_ID добавлено в инцидент R-Vision SOAR (см. рисунки по ссылкам ниже).

Поле ALERT_ID в R-Vision SOAR версии 4.0



Добавление поля ALERT_ID в R-Vision SOAR версии 4.0

Поле ALERT_ID в R-Vision SOAR версии 5.0



Добавление поля ALERT_ID в R-Vision SOAR версии 5.0

Чтобы добавить в R-Vision SOAR поле инцидента ALERT_URL:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.

2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.

3. В поле **Наименование** введите название поля, например `Alert URL`.

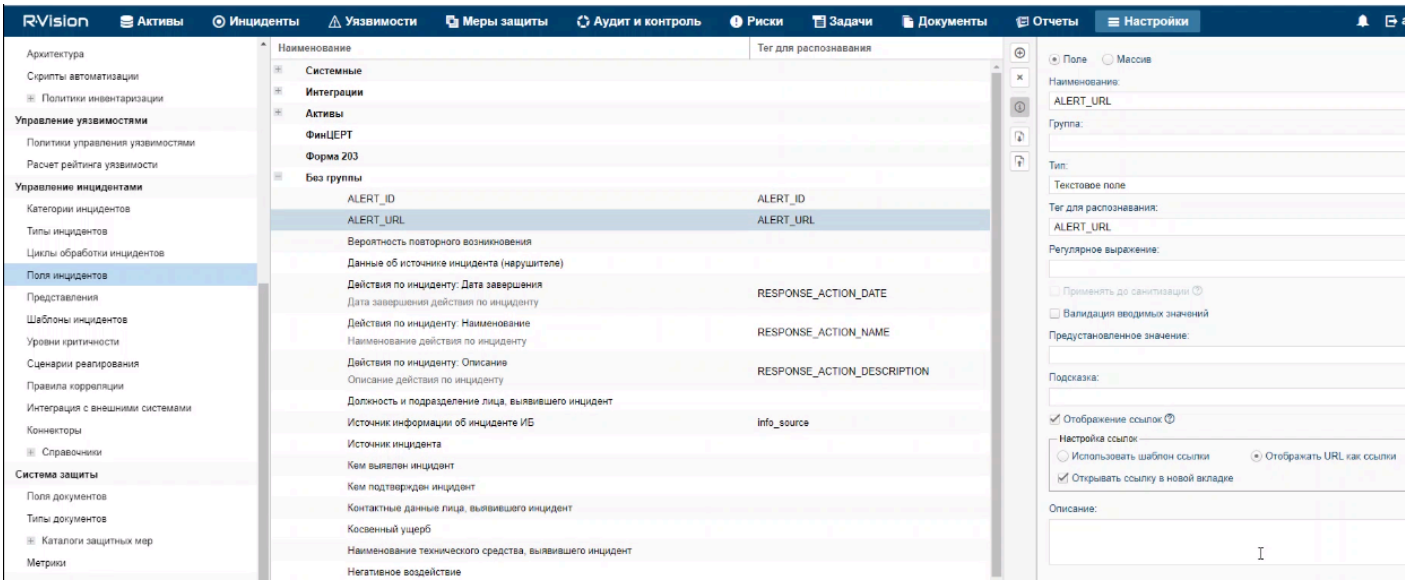
4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.

5. В поле **Тег для распознавания** введите `ALERT_URL`.

6. Установите флажки **Отображение ссылок** и **Отображать URL как ссылки**.

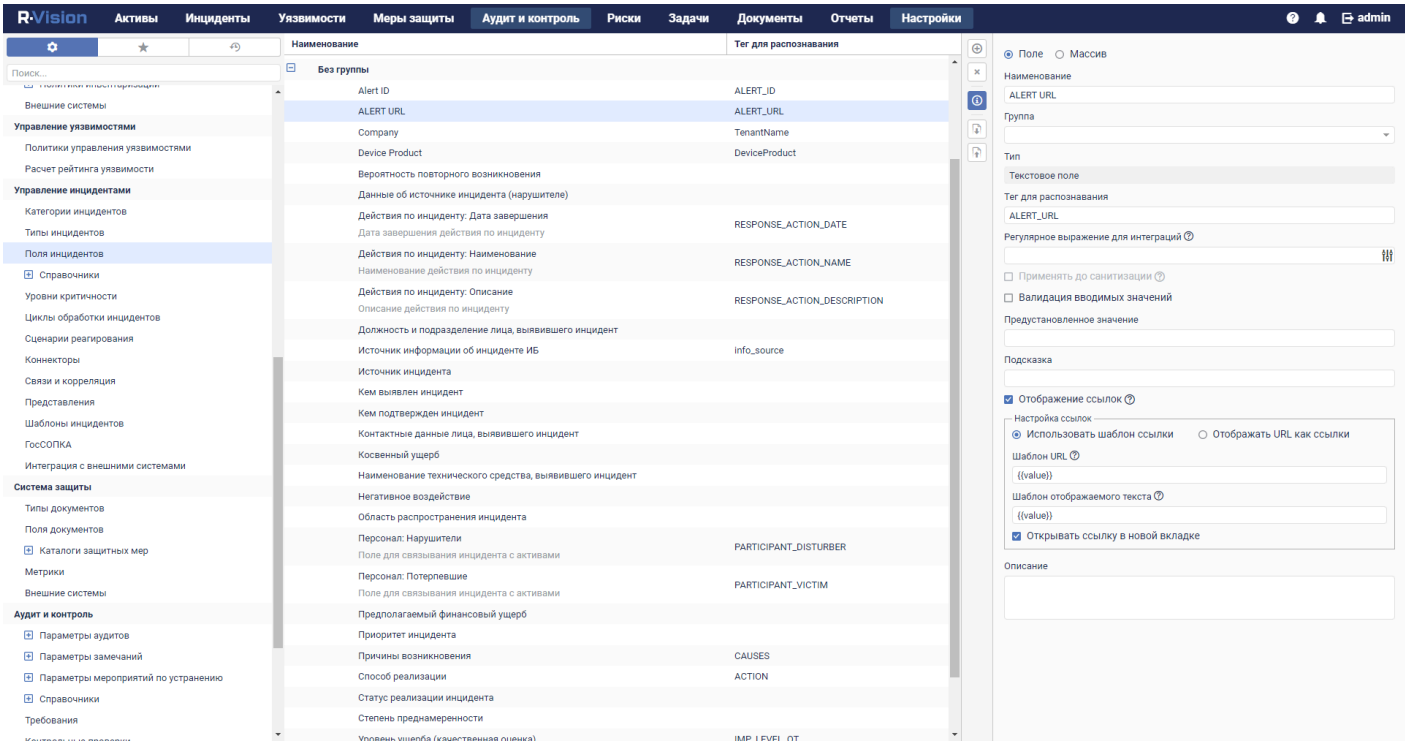
Поле ALERT_URL добавлено в инцидент R-Vision SOAR (см. рисунки по ссылкам ниже).

Поле ALERT_URL в R-Vision SOAR версии 4.0



Добавление поля ALERT_URL в R-Vision SOAR версии 4.0

Поле ALERT_URL в R-Vision SOAR версии 5.0



Добавление поля ALERT_URL в R-Vision SOAR версии 5.0

При необходимости аналогичным образом можно настроить отображение других данных из алерта KUMA в инциденте R-Vision SOAR.

Создание коллектора в R-Vision SOAR

Чтобы создать коллектор в R-Vision SOAR:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Общие** → **Коллекторы** нажмите на значок плюса.

2. В поле **Название** укажите название коллектора (например, `Main collector`).

3. В поле **Адрес коллектора** введите IP-адрес или название хоста, где установлена R-Vision SOAR (например, `127.0.0.1`).

4. В поле **Порт** введите значение `3001`.

5. Нажмите **Добавить**.

6. На вкладке **Организации** выберите организацию, для которой вы хотите добавить интеграцию с KUMA и установите флажки **Коллектор по умолчанию** и **Коллектор реагирования**.

Коллектор R-Vision SOAR создан.

Создание коннектора в R-Vision SOAR

Чтобы создать коннектор в R-Vision SOAR:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** нажмите на значок плюса.

2. В раскрывающемся списке **Тип** выберите **REST**.

3. В поле **Название** укажите название коннектора, например, `KUMA`.

4. В поле **URL** введите API-запрос на закрытие алерта в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

   Пример: `https://kuma.example.com:7223/api/v1/alerts/close`

5. В раскрывающемся списке **Тип авторизации** выберите **Токен**.

6. В поле **Auth header** введите значение `Authorization`.

7. В поле **Auth value** введите токен главного администратора KUMA в следующем формате:

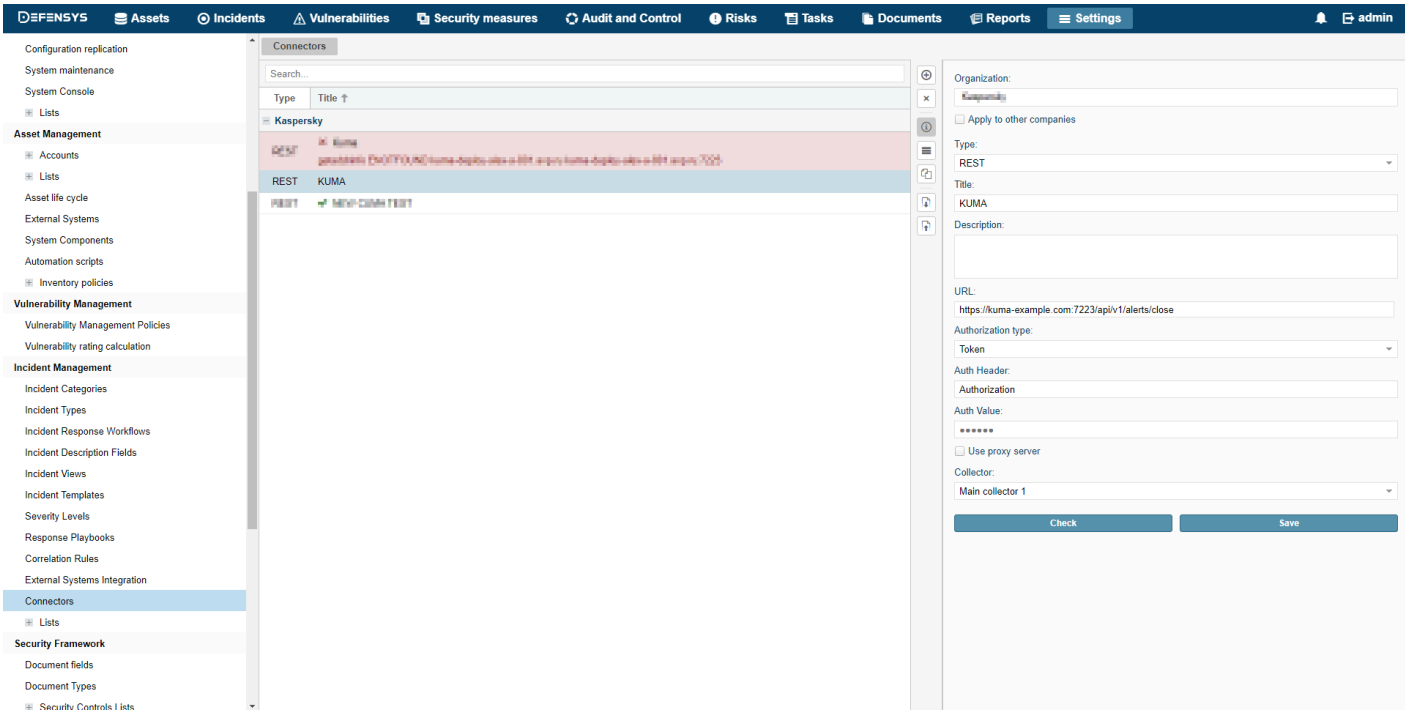
   `Bearer <токен главного администратора KUMA>`

8. В раскрывающемся списке **Коллектор** выберите ранее созданный коллектор.

9. Нажмите **Сохранить**.

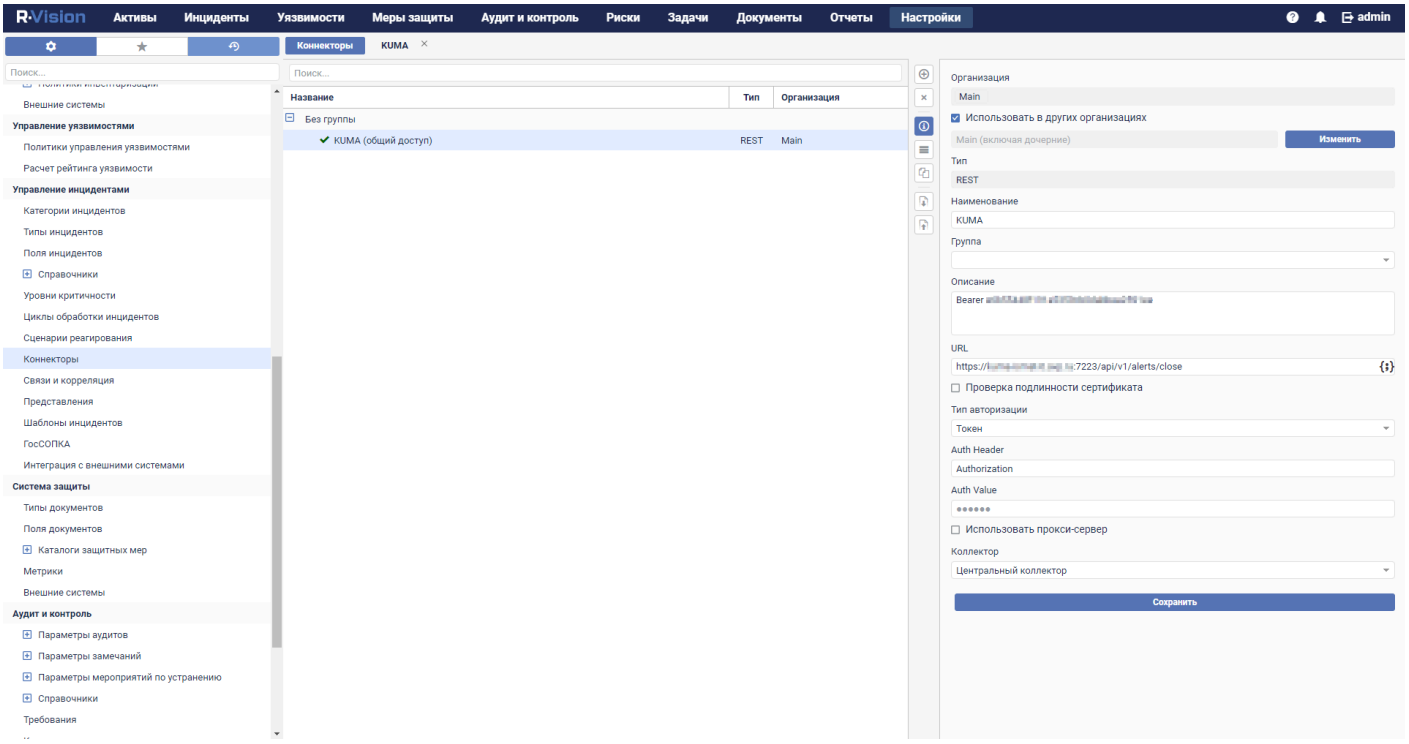
Коннектор создан (см. рисунки по ссылкам ниже).

Коннектор в R-Vision SOAR версии 4.0



Коннектор в R-Vision SOAR версии 4.0

Коннектор в R-Vision SOAR версии 5.0



Коннектор в R-Vision SOAR версии 5.0

После того как коннектор создан, требуется настроить отправку API-запросов на закрытие алертов в KUMA.

Чтобы настроить отправку API-запросов в R-Vision SOAR:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** откройте созданный коннектор для редактирования.

2. В раскрывающемся списке типа запросов выберите **POST**.

3. В поле **Params** введите API-запрос на закрытие алерта в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

   Пример, `https://kuma.example.com:7223/api/v1/alerts/close`

4. На вкладке **HEADERS** добавьте следующие ключи и их значения:

   - Ключ `Content-Type`; значение: `application/json`.

   - Ключ `Authorization`; значение: `Bearer <токен главного администратора KUMA>`.

     Токен главного администратора KUMA можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.

5. На вкладке **BODY** → **Raw** введите содержание тела API-запроса:

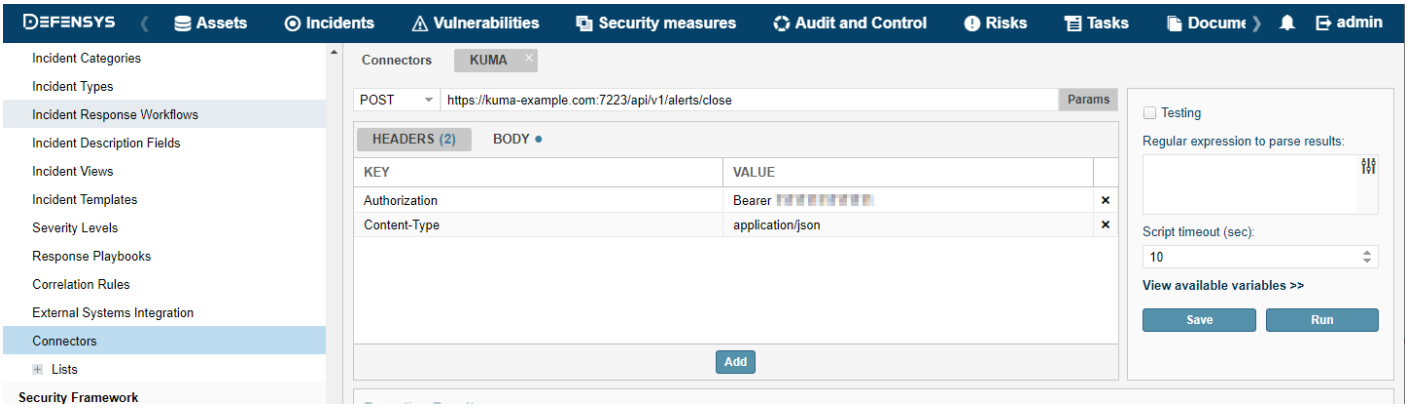
```
{
    "id":"{{tag.ALERT_ID}}",
    "reason":"<причина закрытия алерта. Доступные значения: "Incorrect Correlation Rule", "Incorrect Data", "Responded".>"
```

```
}
```

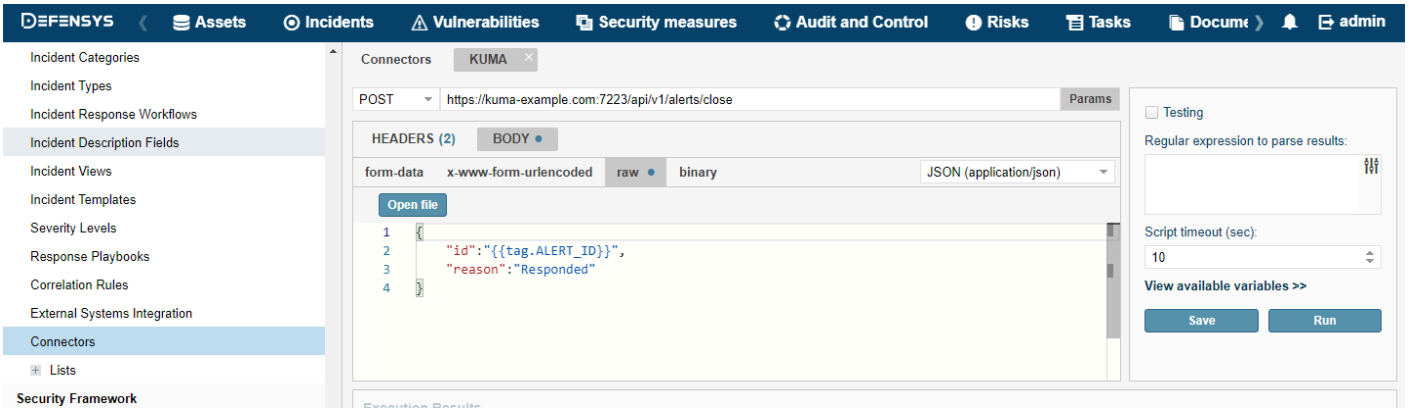
6. Нажмите **Сохранить**.

Коннектор настроен (см. рисунки по ссылкам ниже).

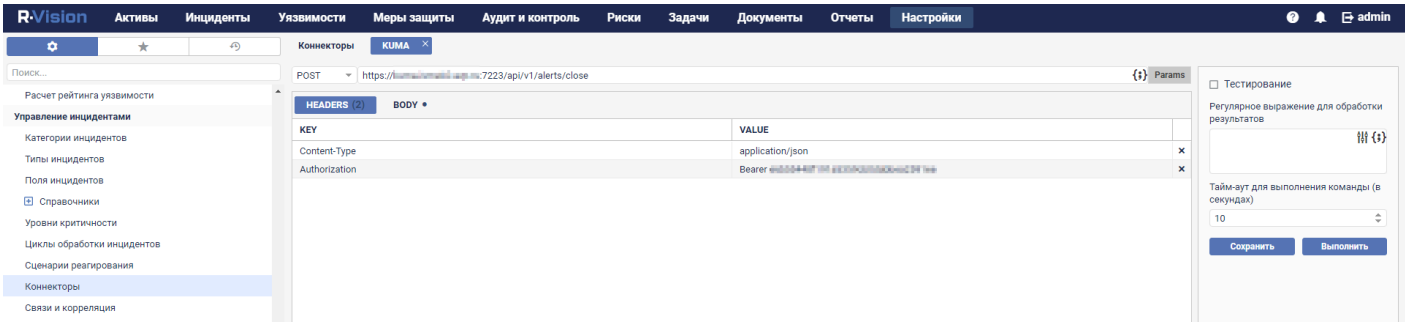
Коннектор в R-Vision SOAR версии 4.0



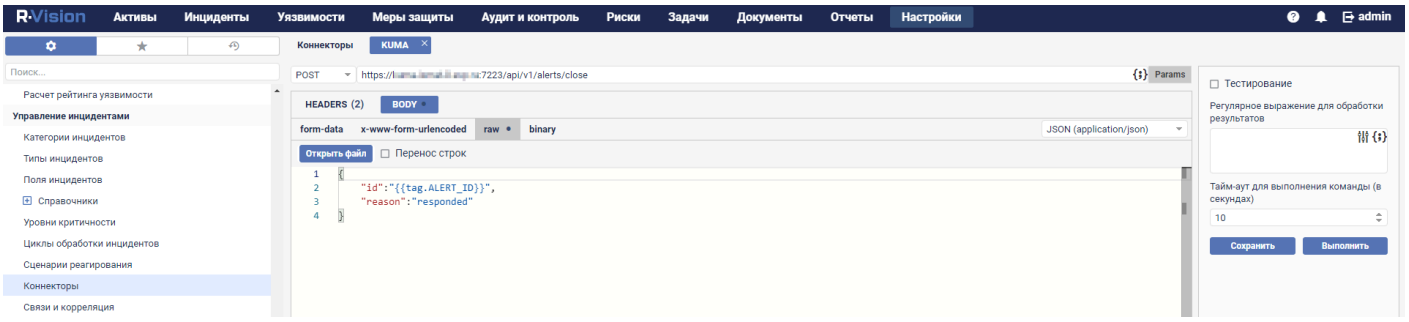
Заголовок API-запроса



Тело API-запроса



Заголовок API-запроса



Тело API-запроса

Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision SOAR

Чтобы создать правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision SOAR:

1. В веб-интерфейсе R-Vision SOAR в разделе **Настройки** → **Управление инцидентами** → **Сценарии реагирования** нажмите на значок плюса.

2. В поле **Название** введите название создаваемого правила, например `Close alert`.

3. В раскрывающемся списке **Группа** выберите **Все сценарии**.

4. В блоке параметров **Критерии автоматического запуска** нажмите **Добавить** и в открывшемся окне введите условия срабатывания правила:

   a. В раскрывающемся списке **Тип** выберите **Значение поля**.

   b. В раскрывающемся списке **Поле** выберите **Статус инцидента**.

   c. Установите флажок напротив статуса **Закрыт**.

   d. Нажмите **Добавить**.

   Условия срабатывания правила добавлены. Правило будет срабатывать при закрытии инцидента.

5. В блоке параметров **Действия по инциденту** нажмите **Добавить** → **Запуск коннектора** и в открывшемся окне выберите коннектор, который следует выполнить при срабатывании правила:

   a. В раскрывающемся списке **Коннектор** выберите ранее созданный коннектор.

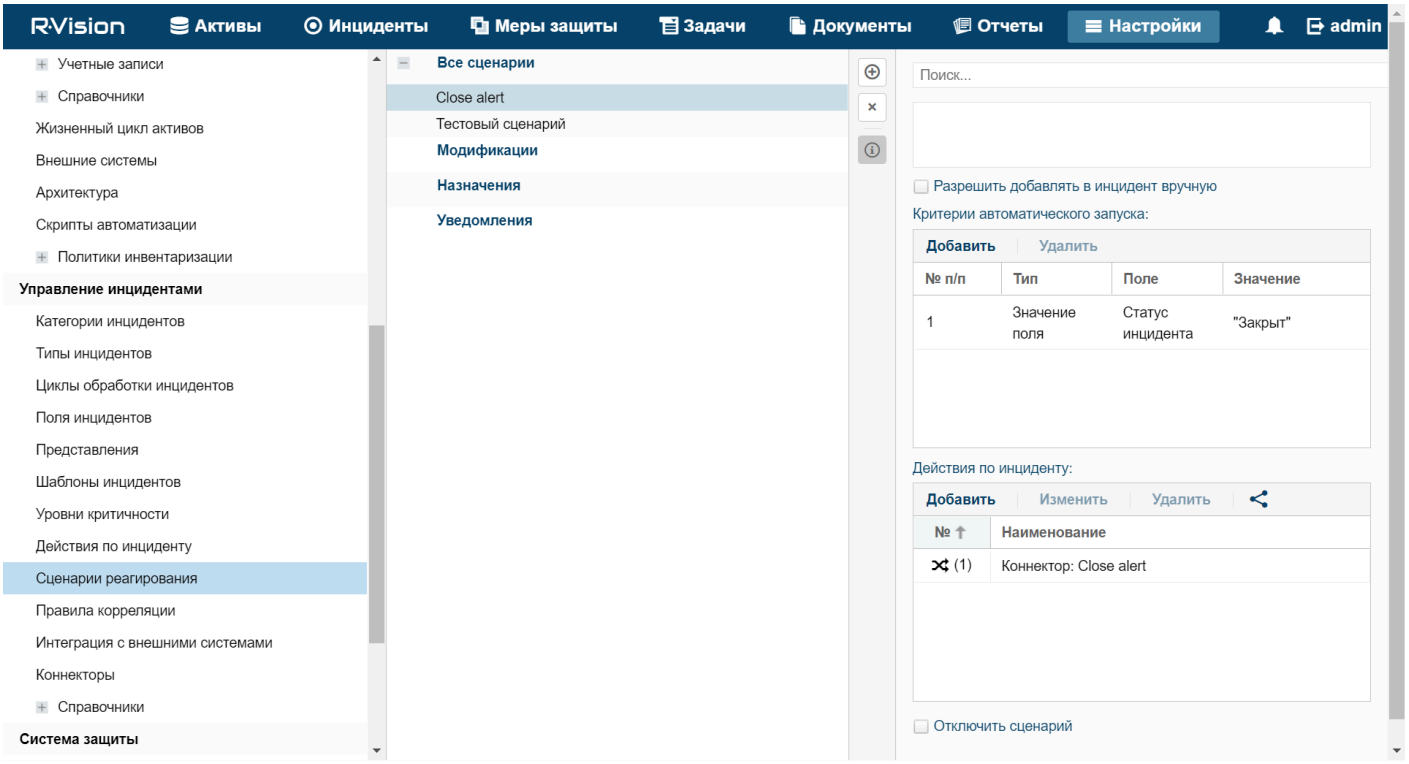
   b. Нажмите **Добавить**.

   Коннектор добавлен в правило.

6. Нажмите **Добавить**.

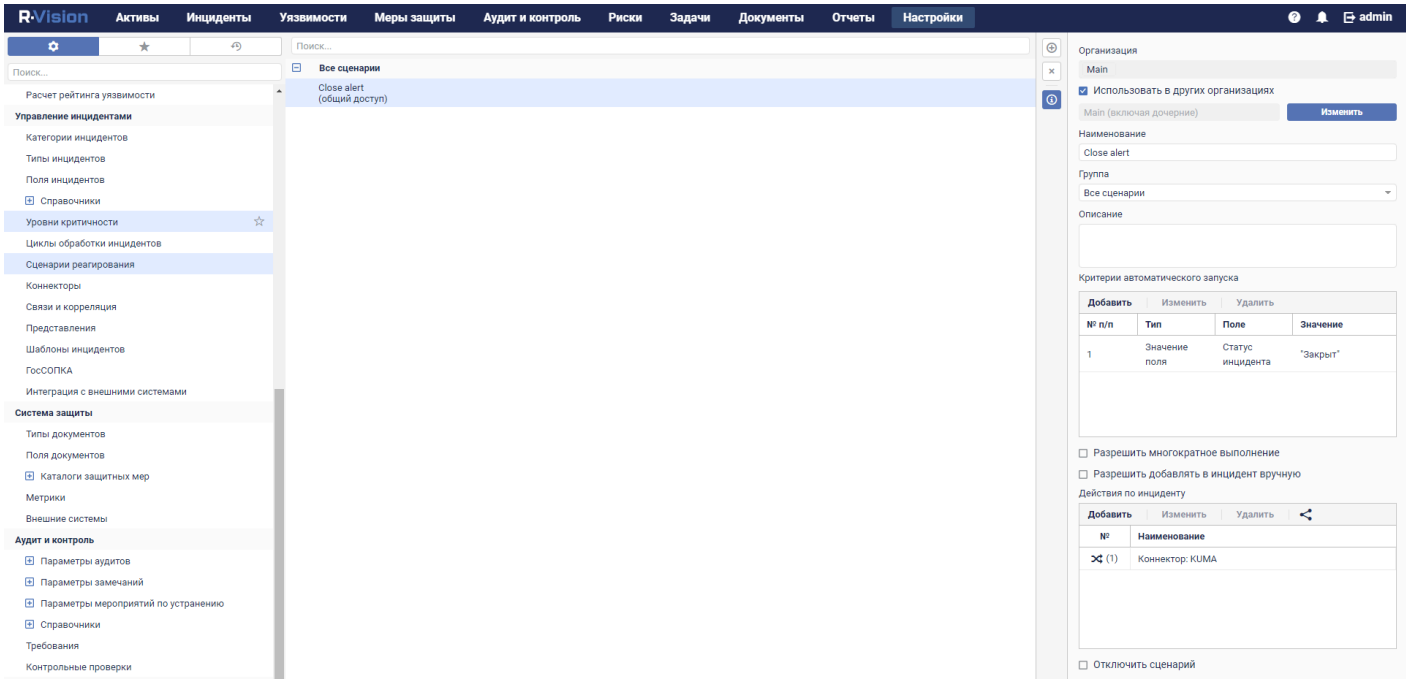
Правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision SOAR создано (см. рисунки по ссылкам ниже).

Правило сценария R-Vision SOAR версии 4.0



Правило сценария R-Vision SOAR версии 4.0

Правило сценария R-Vision SOAR версии 5.0



Правило сценария R-Vision SOAR версии 5.0

Работа с алертами с помощью R-Vision SOAR

После того как интеграция KUMA и R-Vision SOAR настроена, данные об алертах KUMA поступают в R-Vision SOAR. Изменение параметров алертов в KUMA отражается в R-Vision SOAR. Изменение статусов алертов в KUMA или R-Vision SOAR, кроме закрытия, также отражается в другой системе.

Если настроена интеграция KUMA и R-Vision SOAR, вы можете выполнять следующее:

- **Передавать сведения о киберугрозах из KUMA в R-Vision SOAR**

  Из KUMA в R-Vision SOAR автоматически передаются сведения об обнаруженных алертах. При этом в R-Vision SOAR создается инцидент.

  В R-Vision SOAR передаются следующие сведения об алерте KUMA:

  - идентификатор;
  - название;
  - статус;
  - дата первого события, относящегося к алерту;
  - дата последнего обнаружения, относящегося к алерту;
  - имя учетной записи или адрес электронной почты специалиста по безопасности, назначенного для обработки алерта;
  - уровень важности алерта;
  - категория инцидента R-Vision SOAR, соответствующего алерту KUMA;
  - иерархический список событий, связанных с алертом;

- список активов, как внутренних, так и внешних, связанных с алертом;
- список пользователей, связанных с алертом;
- журнал изменений алерта;
- ссылка на алерт в KUMA.

- **Расследовать киберугрозы в KUMA**

  Первоначальная обработка алерта производится в KUMA. Специалист по безопасности может уточнять и менять любые параметры алерта, кроме идентификатора и названия. Внесенные изменения отражаются в карточке инцидента R-Vision SOAR.

  Если киберугроза признается ложной и алерт закрывается в KUMA, соответствующий ему инцидент R-Vision SOAR также автоматически закрывается.

- **Закрывать инциденты в R-Vision SOAR**

  После необходимых работ по инциденту и фиксации хода расследования в R-Vision SOAR инцидент закрывается. Соответствующий алерт KUMA также автоматически закрывается.

- **Открывать ранее закрытые инциденты**

  Если в процессе мониторинга обнаруживается, что инцидент не был решен полностью или обнаруживаются дополнительные сведения, такой инцидент снова открывается в R-Vision SOAR. При этом в KUMA алерт остается закрытым.

  Специалист по безопасности с помощью ссылки может перейти из инцидента R-Vision SOAR в соответствующий алерт в KUMA и изменить его параметры, кроме идентификатора, названия и статуса. Внесенные изменения отражаются в карточке инцидента R-Vision SOAR.

  Дальнейший анализ происходит в R-Vision SOAR. Когда расследование завершено и инцидент в R-Vision SOAR снова закрыт, статус соответствующего алерта в KUMA не меняется: алерт остается закрытым.

- **Запрашивать дополнительные сведения из системы-источника в рамках сценария реагирования или вручную**

  Если в процессе анализа в R-Vision SOAR возникает необходимость получить дополнительные сведения из KUMA, в R-Vision SOAR можно сформировать требуемый поисковый запрос (например, запрос телеметрии, репутации, сведений о хосте) к KUMA. Запрос передается с помощью REST API KUMA, ответ фиксируется в карточке инцидента R-Vision SOAR для дальнейшего анализа и вывода в отчет.

  Действия выполняются в такой же последовательности на этапе автоматической обработки, если нет возможности сразу сохранить всю информацию по инциденту при импорте.

Интеграция с Active Directory, Active Directory Federation Services и FreeIPA

KUMA можно интегрировать с используемыми в вашей организации службами Active Directory®, Active Directory Federation Services и FreeIPA.

Вы можете настроить подключение к службе каталогов Active Directory по протоколу LDAP. Это позволит использовать информацию из Active Directory в правилах корреляции для обогащения событий и алертов, а также для аналитики.

Если вы настроите соединение с сервером контроллера домена, это позволит использовать доменную авторизацию. В этом случае вы сможете привязать группы пользователей из домена к фильтрам ролей KUMA. Пользователи, принадлежащие к этим группам, смогут войти в веб-интерфейс KUMA, используя свои доменные учетные данные, и получат доступ к разделам решения в соответствии с назначенной ролью.

> Рекомендуется предварительно создать в Active Directory, Active Directory Federation Services или FreeIPA группы пользователей, которым вы хотите предоставить возможность проходить авторизацию с помощью доменной учетной записи в веб-интерфейсе KUMA. В свойствах учетной записи пользователя в Active Directory обязательно должен быть указан адрес электронной почты.

Подключение по протоколу LDAP

Подключения по протоколу LDAP создаются и управляются в разделе **Параметры** → **Интеграции** → **LDAP-сервер** веб-интерфейса KUMA. 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`
- `company`
- `department`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `ipaUniqueID`
- `l`

- `mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`
- `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 выключить все LDAP-подключения тенанта:

1. Откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить все подключения к LDAP.

2. Выполните одно из следующих действий:

   a. Переведите переключатель в столбце **Статус** в положение **Включено** или **Выключено**.

   b. Нажмите на имя тенанта в столбце **Тенант** и в открывшейся боковой панели **Интеграция с LDAP-сервером** сделайте следующее:

      - Переведите переключатель **Статус** в положение **Включено** или **Выключено**.

      - Нажмите **Сохранить**.

Чтобы включить или выключить определенное LDAP-подключение:

1. Откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить все подключения к LDAP.

2. Нажмите на имя тенанта в столбце **Тенант** и в открывшейся боковой панели **Интеграция с LDAP-сервером** перейдите к блоку **Подключения**.

3. С помощью переключателя в столбце **Статус** включите или выключите определенное LDAP-подключение.

4. Нажмите **Сохранить**.

Добавление тенанта в список тенантов для интеграции с LDAP-сервером

Чтобы добавить тенант в список тенантов для интеграции с LDAP-сервером:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** →**LDAP-сервер**.

   Отобразится таблица **Интеграция с LDAP-сервером по тенантам**.

2. Нажмите на кнопку **Добавить параметры для нового тенанта**.

   Справа откроется панель **Интеграция с LDAP-сервером**.

3. В раскрывающемся списке **Тенант** выберите тенант, который нужно добавить.

4. Нажмите **Добавить**.

Выбранный тенант будет добавлен в список тенантов для интеграции с LDAP-сервером.

Чтобы удалить тенант из списка тенантов для интеграции с LDAP-сервером:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** →**LDAP-сервер**.

   Отобразится таблица **Интеграция с LDAP-сервером по тенантам**.

2. Установите флажок рядом с тенантом, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. Подтвердите удаление тенанта.

Выбранный тенант будет удален из списка тенантов для интеграции с LDAP-сервером.

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер**.

2. Выберите или добавьте тенант, для которого хотите создать подключение к LDAP.

3. В панели **Интеграция с LDAP-сервером по тенантам** выберите тенант из списка или добавьте тенант по кнопке **Добавить параметры для нового тенанта**, для которого вы хотите создать подключение к LDAP.

4. В блоке параметров **Подключения** нажмите на кнопку **Создать**.

   Откроется панель **Создать подключения**.

5. Если хотите использовать это LDAP-подключение, с помощью переключателя **Состояние** включите подключение.

6. Укажите уникальное название LDAP-подключения. Длина должна быть от 1 до 128 символов в кодировке Unicode.

7. В раскрывающемся списке выберите секрет с учетными данными для подключения к серверу Active Directory. Для этого выполните одно из следующих действий:

   - Если вы создали секрет ранее, в раскрывающемся списке **Секрет** выберите существующий секрет типа **credentials**.

   - Если вы хотите создать секрет, нажмите **Создать**.

     Откроется панель **Создание секрета**.

     1. В поле **Название** введите название секрета. Оно должно содержать от 1 до 128 символов в кодировке Unicode.

     2. В полях **Пользователь** и **Пароль** 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>`.

     3. При необходимости в раскрывающемся списке **Теги** выберите теги для секрета.

     4. При необходимости в поле **Описание** введите описание секрета (до 4000 символов в кодировке Unicode).

     5. Нажмите на кнопку **Создать**.

8. В поле **URL** введите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

При необходимости с помощью кнопки **Добавить** укажите адреса нескольких серверов с контроллерами домена, которые могут потребоваться в случае недоступности одного из серверов. Все указанные серверы должны находиться в одном домене. В одном поле можно указать только один сервер с контроллером домена. Если первый контроллер домена недоступен, система подключается к следующему в списке, а затем к следующему, пока не установит соединение.

Если при попытке подключения хост контроллера домена не будет найден, например если в поле **URL** введен несуществующий адрес, переключения к следующему адресу контроллера домена не произойдет. Вместо этого KUMA вернет ошибку.

9. Выберите один из следующих типов TLS-шифрования для соединения с контроллером домена:

   - **LDAPS**.

     При использовании LDAPS сразу устанавливается шифрованное соединение по порту 636. Этот тип TLS-шифрования установлен по умолчанию.

   - **startTLS**.

     При использовании 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.

   - **Незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

10. В раскрывающемся списке **Сертификат** укажите TLS-сертификат, аккредитованного центра сертификации, которым подписан сертификат LDAP-сервера. Невозможно использовать пользовательские сертификаты.

    Для этого выполните одно из следующих действий:

    - Если у вас уже есть сертификат, выберите его в раскрывающемся списке.

    - Если вы хотите создать сертификат, нажмите **Создать**.

      Откроется панель **Создание секрета**.

      a. В поле **Название** введите название, которое будет отображаться в списке сертификатов.

      b. Нажмите на кнопку **Загрузить сертификат**, чтобы добавить файл с сертификатом Active Directory.

      Поддерживаются открытые ключи сертификата X.509 в кодировке Base64.

      c. При необходимости в раскрывающемся списке **Теги** выберите теги для сертификата.

      d. При необходимости в поле **Описание** введите описание сертификата.

      e. Нажмите на кнопку **Создать**.

      Сертификат будет загружен и отобразится в списке **Сертификат**.

    > Поле **Сертификат** не является обязательным, если вы выбрали тип TLS-шифрования **Незащищенный**.

11. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

    Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, решение обратится к следующему указанному серверу. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

12. В поле **База поиска (Base DN)** введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.

13. В поле **Пользовательские поля учетных записей AD** укажите дополнительные атрибуты, с использованием которых вы хотите обогащать события.

    Как указать дополнительные атрибуты

    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.

       Список ипортируемых атрибутов из AD

       Из Active Directory можно запросить следующие атрибуты учетных записей:

       - `accountExpires`
       - `badPasswordTime`
       - `cn`
       - `company`
       - `department`
       - `displayName`
       - `distinguishedName`
       - `division`
       - `employeeID`
       - `ipaUniqueID`
       - `l`
       - `mail`
       - `mailNickname`
       - `managedObjects`

- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`
- `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 для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. 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.

14. Нажмите на кнопку **Создать**.

    Если во время создания подключения тенант был удален, кнопка **Создать** остается активной, но при попытке создать подключение отобразится сообщение об ошибке. Удаленный тенант будет отображаться в списке доступных тенантов до тех пор, пока вы не обновите страницу, нажав на клавишу **F5**.

LDAP-подключение к Active Directory будет создано и отобразится в панели **Интеграция с LDAP-сервером**.

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. Иначе 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 для другого тенанта, скопировав уже существующее подключение. В этом случае в созданное подключение дублируются все параметры исходного подключения.

Чтобы скопировать LDAP-подключение:

1. Откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, для которого вы хотите скопировать подключение к LDAP.

2. Выберите нужное подключение и нажмите на кнопку **Добавить параметры для нового тенанта**.

3. В открывшемся окне **Интеграция с LDAP-сервером** в раскрывающемся списке **Тенант** выберите тенанта, для которого вы хотите создать копию подключения.

4. Нажмите на кнопку **Запустить задачу импорта**.

5. 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 веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. Выберите тенант, для которого вы хотите изменить подключение к LDAP-серверу.

   Справа откроется панель **Интеграция с LDAP-сервером**.
3. Нажмите на подключение к LDAP-серверу, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к LDAP-серверу.
4. Измените значения необходимых параметров.
5. Нажмите на кнопку **Сохранить**.

   Подключение к LDAP-серверу будет изменено.
6. Перезапустите сервисы KUMA, использующие обогащение данными LDAP-серверов, чтобы изменения вступили в силу.

Изменение частоты обновления данных

KUMA обращается к LDAP-серверу для обновления данных об учетных записях. Это происходит в следующих случаях:

- Сразу после создания 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 разделе **Диспетчер задач** веб-интерфейса KUMA.

Чтобы изменить расписание обращений KUMA к LDAP-серверам:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. В окне **Интеграция с LDAP-сервером по тенантам** выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. В поле **Интервал обновления данных (час.)** укажите требуемую частоту в часах. Значение по умолчанию – 12.

Расписание обращений будет 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 веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. В окне **Интеграция с LDAP-сервером по тенантам** выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. 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. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. В окне **Интеграция с LDAP-сервером по тенантам** выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Нажмите на кнопку **Запустить задачу импорта**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача на получение данныхоб учетных записях выбранного тенанта.

Чтобы запустить задачу на обновление данных об учетных записях для одного LDAP-подключения тенанта:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. В окне **Интеграция с LDAP-сервером по тенантам** выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. В блоке **Подключения** выберите требуемое подключение к LDAP-серверу.
4. В открывшемся окне нажмите на кнопку **Запустить задачу импорта**.

В разделе **Диспетчер задач** веб-интерфейса KUMA 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. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Интеграции** → **LDAP-сервер**.
2. В окне **Интеграция с LDAP-сервером по тенантам** выберите нужный тенант.
3. Нажмите на кнопку **Удалить**.
4. Подтвердите удаление подключения.

LDAP-подключение к Active Directory удалено.

Аутентификация с помощью доменных учетных записей

Чтобы пользователи могли проходить аутентификацию в веб-интерфейсе KUMA с помощью своих доменных учетных данных, требуется выполнить следующие этапы настройки.

1. **Включить доменную аутентификацию**

   По умолчанию доменная аутентификация выключена, а подключение к домену не настроено.
2. **Настроить соединение с контроллером домена**

   Доступны следующие соединения:

   - Active Directory (AD)
   - Active Directory Federation Services (ADFS)
   - FreeIPA

   Одновременно могут быть настроены параметры подключения к AD и ADFS.

   Подключение возможно только к одному домену.
3. **Добавить группы ролей пользователей**

   Вы можете указать для каждой роли KUMA группу домена. Пользователи из этой группы, пройдя аутентификацию с помощью своих доменных учетных данных, будут получать доступ к веб-интерфейсу KUMA в соответствии с указанной ролью.

При этом решение проверяет соответствие группы пользователя указанному фильтру в порядке следования ролей в веб-интерфейсе KUMA: Младший аналитик → Аналитик первого уровня → Аналитик второго уровня → Администратор тенанта → Главный администратор. При первом совпадении пользователю присваивается роль и дальнейшая проверка не осуществляется. Если для пользователя указано две группы в одном тенанте, то будет использована роль с наибольшими правами. Если указано несколько групп для разных тенантов, то в каждом тенанте пользователю будет присвоена указанная роль.

При нажатии на **Тенант**:

- под тенантом раскрывается весь список ролей и групп, принадлежащих данному тенанту.
- под строкой, которая содержит название тенанта, общее количество ролей и общее количество групп, принадлежащее данному тенанту, отображаются строки, которые содержат название тенанта, название роли и название группы.
- дубликаты названий ролей и групп объединяются при копировании и добавлении фильтра (то есть, если одному тенанту принадлежит в таблице запись **роль младший аналитик, группа 1**, то при попытке добавить или скопировать такую же запись (**роль младший аналитик**, **группа 1**) от другого тенанта запись в гриде **младший аналитик**, **группа 1** будет только в единичном экземпляре, без дублирования.
- роли отображаются в отсортированном виде сверху вниз от старшей роли к младшей.

Вы можете скопировать настроенные роли пользователей и соответствующие им группы в другой тенант. Для этого установите рядом с ними флажок и нажмите на кнопку **Скопировать в тенант**. В открывшемся окне отобразится список доступных тенантов. При копировании ролей пользователей вы можете сделать следующее:

- Выбрать одну или несколько ролей внутри одного тенанта для копирования параметров.
- Скопировать весь тенант с настроенными ролями и группами.
- Скопировать параметры сразу в несколько тенантов, но только из одного. В списке доступных тенантов будут недоступны тенант Shared и тенант, из которого вы копируете.

Все доменные пользователи при первой аутентификации получают доступ к набору пространств по умолчанию, который указан в разделе **Доступ к пространствам**.

При необходимости вы можете удалить сразу несколько тенантов или ролей пользователей с их группами. Для этого нужно установить флажок рядом с необходимыми сущностями и нажать на кнопку **Удалить**. Вы можете удалять выбранные роли как внутри одного тенанта, так и одновременно из разных.

Особенности входа в систему после настройки доменной аутентификации

Для успешной аутентификации необходимо соблюдать следующие условия:

- **FreeIPA**: при входе в систему пользователю следует указывать в логине домен заглавными буквами. Пример: user@FREEIPA.COM.
- **AD/ADFS**: при входе в систему пользователю следует указывать в логине UserPrincipalName. Пример: user@domain.ru.

Если вы выполнили все этапы настройки, но пользователь не может пройти аутентификацию в веб-интерфейсе KUMA с помощью своей доменной учетной записи, мы рекомендуем проверить конфигурацию на наличие следующих проблем:

- В свойствах учетной записи пользователя в Active Directory не указан адрес электронной почты. В этом случае при первой аутентификации пользователя отобразится сообщение об ошибке и учетная запись KUMA не будет создана.
- Локальная учетная запись KUMA с адресом электронной почты, указанным в свойствах доменной учетной записи, уже существует. В этом случае при попытке аутентификации с помощью доменной учетной записи пользователь получит сообщение об ошибке.
- Доменная аутентификация отключена в параметрах KUMA.
- Допущена ошибка при вводе группы ролей.
- Доменное имя пользователя содержит пробел.

[▷]

https://rutube.ru/video/8cabd9b4a160f875fa2ef1abbd286e5d/

Включение и выключение доменной аутентификации

По умолчанию доменная аутентификация выключена. Чтобы ее включить, необходимо перевести переключатель **Состояние** в активное положение. Если после настройки подключения вы хотите временно приостановить доменную аутентификацию, вы можете выключить ее в веб-интерфейсе KUMA, не удаляя заданные ранее значения параметров. При необходимости вы сможете в любой момент включить аутентификацию снова.

Чтобы включить или выключить доменную авторизацию пользователей в веб-интерфейсе KUMA:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.
2. В раскрывающемся списке **Тип аутентификации** выберите один из вариантов:
   - **AD/ADFS**.
   - **FreeIPA**.

3. Выполните одно из следующих действий:

   - Если вы хотите включить доменную аутентификацию, включите переключатель **Состояние**.
   - Если вы хотите выключить доменную аутентификацию, выключите переключатель **Состояние**.

4. Нажмите на кнопку **Сохранить**.

Выбранные параметры будут сохранены и применены.

Настройка соединения KUMA с FreeIPA

Вы можете подключиться только к одному домену FreeIPA. Для этого требуется настроить соединение с контроллером домена.

Чтобы настроить соединение с контроллером домена FreeIPA:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.
2. В раскрывающемся списке **Тип аутентификации** выберите **FreeIPA**.
3. В блоке параметров **FreeIPA** включите переключатель **Состояние**.
4. В поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов FreeIPA. Формат записи: dc=example,dc=com.
5. В поле **URL** укажите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

   Вы можете указать через запятую адреса до трех серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

6. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Режим TLS** 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.

   - **LDAPS**.

     При использовании LDAPS сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

7. Если включено TLS-шифрование, поле **Секрет** становится обязательным для заполнения и в нем требуется указать секрет с типом certificate. Если вы загрузили секрет ранее, выберите его в раскрывающемся списке **Секрет.** При необходимости, создайте новый секрет с типом certificate с помощью кнопки + и выберите секрет в раскрывающемся списке.

8. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена. По умолчанию указано значение 0.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, решение будет обращаться к следующему указанному серверу. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

9. В раскрывающемся списке **Секрет пользовательской интеграции** выберите секрет с типом credentials.

   Если вы хотите загрузить новый секрет с типом credentials, справа от списка **Секрет пользовательской интеграции** нажмите на кнопку +. В открывшемся окне **Секрет** в поле **Название** введите название секрета, которое будет отображаться в списке после сохранения. В поле **Пользователь** укажите DistinguishedName в следующем формате: uid=admin,cn=users,cn=accounts,dc=ipa,dc=test. Укажите **Пароль** и нажмите на кнопку **Сохранить**.

   Секрет будет загружен и станет доступен для выбора в раскрывающемся списке **Секрет пользовательской интеграции**.

10. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы FreeIPA, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в KUMA автоматически, поэтому их не нужно добавлять отдельно.

    > В случае когда для пользователя указано несколько групп в одном тенанте, будет использована роль с наибольшими правами и дополнительные роли, если дополнительные роли были назначены.

    Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

11. Нажмите на кнопку **Сохранить**.

Соединение с контроллером домена FreeIPA будет настроено.

Вы также можете проверить соединение для введенных ранее параметров соединения с контроллером домена.

Чтобы проверить соединение с контроллером домена:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **FreeIPA**.

3. В блоке параметров **FreeIPA** выберите нужный секрет в поле **Данные аутентификации**.

   При необходимости вы можете создать новый секрет, нажав на кнопку +, или изменить параметры существующего секрета, нажав на кнопку ✎. Если интеграция с FreeIPA включена, выбор секрета всегда сбрасывается при загрузке страницы, даже

4. Нажмите на кнопку **Тест**.

   После нажатия на кнопку **Тест** система выполнит проверку соединения с доменом и вернет всплывающее уведомление с результатами теста. Система не выполняет проверку возможности входа в систему и правильность настройки группы пользователей.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

> Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.
2. В блоке параметров **Группы администрирования** нажмите на кнопку **Добавить группу**.
3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.
4. В раскрывающемся списке **Роли** укажите роли для пользователя. Можно выбрать несколько ролей. Доступны следующие значения:
   - **Администратор тенанта**.
   - **Аналитик второго уровня**.
   - **Аналитик первого уровня**.
   - **Младший аналитик**.
   - **Доступ к общим панелям мониторинга**. Роль доступна только при выборе тенанта Shared в раскрывающемся списке **Тенант**. Для тенанта Shared это единственная роль, которую можно добавить через параметры доменной аутентификации.

   После того как вы выберете роли, для каждой роли появится поле фильтра для группы. Укажите полный путь к группе домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для каждой роли. Пример ввода группы: `CN=KUMA team`, `OU=Groups`, `OU=Clients`, `DC=test`, `DC=domain`.

   Для каждого тенанта можно задать отдельный набор фильтров для ролей.

   Если для какой-то из ролей не указан фильтр, это означает что для данной роли не указаны условия создания учетной записи через доменную аутентификацию. Выполнить аутентификацию с такой ролью невозможно.

   После первой аутентификации пользователей под доменной учетной записью в разделе **Параметры** → **Доступ** → **Пользователи** будут созданы карточки доменных пользователей. Для доменного пользователя в карточке пользователя заблокирована возможность изменения основных ролей (Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик) и доступно добавление и удаление дополнительных ролей (Доступ к КИИ, Работа с НКЦКИ, Чтение общих ресурсов), включая управление привязкой дополнительных ролей к тенантам. Роли назначенные в разделе Доменной аутентификации и назначенные в карточке пользователя дополняют друг друга. Для Главного администратора дополнительные роли в KUMA активированы автоматически, поэтому не нужно добавлять их отдельно. Если доменному пользователю была присвоена роль Главного администратора, а затем роль Главного администратора отозвана, дополнительные роли нужно будет заново присвоить в карточке пользователя в разделе **Параметры** → **Доступ** → **Пользователи**.

   > Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, для каждой группы требуется повторить шаги 2–4, указывая при этом тот же тенант.

5. Если требуется, повторите шаги 2–4 для каждого тенанта, для которого вы хотите настроить доменную аутентификацию с ролями Младший аналитик, Аналитик первого уровня, Аналитик второго уровня или Администратор тенанта.

6. Нажмите на кнопку **Добавить**.

   Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Доступ** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка соединения KUMA с Active Directory

Вы можете подключиться только к одному домену Active Directory. Для этого требуется настроить соединение с контроллером домена.

Чтобы настроить соединение с контроллером домена Active Directory:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **AD/ADFS**.

3. В блоке параметров **Active Directory (AD)** включите переключатель **Состояние**.

4. В поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов Active Directory.

5. В поле **URL** укажите 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.

6. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Режим TLS** 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.

- **LDAPS**.

  При использовании LDAPS сразу устанавливается шифрованное соединение по порту 636.

- **незащищенный**.

При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

7. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат:

   - Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

     Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

   - Если вы хотите загрузить новый сертификат, справа от списка **Секрет** нажмите на кнопку + . В открывшемся окне в поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления. Добавьте файл с сертификатом Active Directory (поддерживаются открытые ключи сертификата X.509 в Base64), нажав на кнопку **Загрузить файл сертификата**. Нажмите на кнопку **Сохранить**.

     Сертификат будет загружен и отобразится в списке **Секрет**.

8. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, решение будет обращаться к следующему указанному серверу. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

9. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в KUMA автоматически и поэтому их не нужно добавлять отдельно.

   > В случае когда для пользователя указано несколько групп в одном тенанте, будет использована роль с наибольшими правами и дополнительные роли, если дополнительные роли были назначены.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

10. Нажмите на кнопку **Сохранить**.

Соединение с контроллером домена Active Directory будет настроено.

Вы также можете проверить соединение для введенных ранее параметров соединения с контроллером домена.

Чтобы проверить соединение с контроллером домена:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **AD/ADFS**.

3. В блоке параметров **Проверка подключения** выберите нужный секрет в поле **Данные аутентификации**.

   При необходимости вы можете создать новый секрет, нажав на кнопку + , или изменить параметры существующего секрета, нажав на кнопку ✎.

В поле **Пользователь** доступны следующие форматы указания пользователя: UserPrincipalName и domain\user.

4. Нажмите на кнопку **Тест**.

   После нажатия на кнопку **Тест** система выполнит проверку соединения с доменом и вернет всплывающее уведомление с результатами теста. Система не выполняет проверку возможности входа в систему и правильность настройки группы пользователей.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

> Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.

2. В блоке параметров **Группы администрирования** нажмите на кнопку **Добавить группу**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.

4. В раскрывающемся списке **Роли** укажите роли для пользователя. Можно выбрать несколько ролей. Доступны следующие значения:

   - **Администратор тенанта**.
   - **Аналитик второго уровня**.
   - **Аналитик первого уровня**.
   - **Младший аналитик**.
   - **Доступ к общим панелям мониторинга**. Роль доступна только при выборе тенанта Shared в раскрывающемся списке **Тенант**. Для тенанта Shared это единственная роль, которую можно добавить через параметры доменной аутентификации.

   После того как вы выберете роли, для каждой роли появится поле фильтра для группы. Укажите полный путь к группе домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для каждой роли. Пример ввода группы: `CN=KUMA team`, `OU=Groups`, `OU=Clients`, `DC=test`, `DC=domain`.

   Для каждого тенанта можно задать отдельный набор фильтров для ролей.

   Если для какой-то из ролей не указан фильтр, это означает что для данной роли не указаны условия создания учетной записи через доменную аутентификацию. Выполнить аутентификацию с такой ролью невозможно.

После первой аутентификации пользователей под доменной учетной записью в разделе **Параметры** → **Доступ** → **Пользователи** будут созданы карточки доменных пользователей. Для доменного пользователя в карточке пользователя заблокирована возможность изменения основных ролей (Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик) и доступно добавление и удаление дополнительных ролей (Доступ к КИИ, Работа с НКЦКИ, Чтение общих ресурсов), включая управление привязкой дополнительных ролей к тенантам. Роли назначенные в разделе Доменной аутентификации и назначенные в карточке пользователя дополняют друг друга. Для Главного администратора дополнительные роли в KUMA активированы автоматически, поэтому не нужно добавлять их отдельно. Если доменному пользователю была присвоена роль Главного администратора, а затем роль Главного администратора отозвана, дополнительные роли нужно будет заново присвоить в карточке пользователя в разделе **Параметры** → **Доступ** → **Пользователи**.

Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, для каждой группы требуется повторить шаги 2–4, указывая при этом тот же тенант.

5. Если требуется, повторите шаги 2–4 для каждого тенанта, для которого вы хотите настроить доменную аутентификацию с ролями Младший аналитик, Аналитик первого уровня, Аналитик второго уровня или Администратор тенанта.

6. Нажмите на кнопку **Добавить**.

Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Доступ** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка соединения KUMA с Active Directory Federation Services

Чтобы настроить доменную аутентификацию в KUMA и обеспечить для пользователей возможность входа в KUMA под учетной записью без указания логина и пароля, необходимо предварительно создать группу подключения и настроить правила на стороне AD FS или убедиться, что необходимые группы подключения и правила уже существуют.

После настройки на странице входа в KUMA появится кнопка **Вход через ADFS**.

Кнопка **Вход через ADFS** будет скрыта на странице входа в KUMA при следующих условиях:

- Если в раскрывающемся списке **Тип аутентификации** выбран пункт **FreeIPA**.
- Если в раскрывающемся списке **Тип аутентификации** выбран пункт **AD/ADFS** и настройки для AD FS отсутствуют или выключен переключатель **Состояние** для настроек AD FS.

Вы можете подключиться только к одному домену ADFS. Для этого требуется настроить соединение с контроллером домена.

Чтобы настроить соединение с контроллером домена AD FS:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** →**Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **AD/ADFS**.

3. В блоке параметров **Active Directory Federation Services (ADFS)** включите переключатель **Состояние**.

4. В поле **Идентификатор клиента** укажите идентификатор KUMA из поля **Client ID** в AD FS.

5. В поле **Идентификатор доверенной стороны** укажите идентификатор KUMA из поля **Relying party identifiers** в AD FS.

6. Укажите **URI для получения метаданных Connect** из поля **Connect Metadata URI**. URI состоит из хоста, на котором расположен AD FS (https://adfs.example.com) и параметра настройки конечной точки (/adfs/.well-known/openid-configuration).

   Например, https://adfs.example.com/adfs/.well-known/openid-configuration.

7. Укажите **URL для перенаправления из ADFS** из поля **Redirect URL** в AD FS. Значение поля **Redirect URL** в AD FS указывается при настройке Application group. В AD FS необходимо указать FQDN KUMA и подстроку </sso-callback>. В KUMA URL необходимо указать без подстроки, например, https://kuma-example:7220.

   В распределенной установке с Ядром KUMA в кластере Raft необходимо настроить балансировщик и затем указать FQDN балансировщика. Например, в параметрах настройки AD FS вам нужно указать https://kuma-load-balancer.com:7220</sso-callback>, а в KUMA в поле **URL для перенаправления из ADFS** вам нужно указать https://kuma-load-balancer.com:7220.

8. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory Federation Services, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в KUMA автоматически, поэтому их не нужно добавлять отдельно.

   > В случае когда для пользователя указано несколько групп в одном тенанте, будет использована роль с наибольшими правами и дополнительными правами, если дополнительные роли были назначены.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

9. Нажмите на кнопку **Сохранить**.

Соединение с контроллером домена Active Directory Federation Services будет настроено.

> Если при попытке входа в KUMA через ADFS пользователю отображается всплывающее сообщение `Access denied` или `Недостаточно прав`, нажмите на кнопку **Сбросить сертификат**. Новый сертификат будет сформирован автоматически.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

> Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе решения выберите раздел **Параметры** → **Доступ** → **Доменная аутентификация**.

2. В блоке параметров **Группы администрирования** нажмите на кнопку **Добавить группу**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.

4. В раскрывающемся списке **Роли** укажите роли для пользователя. Можно выбрать несколько ролей. Доступны следующие значения:

   - **Администратор тенанта**.
   - **Аналитик второго уровня**.
   - **Аналитик первого уровня**.
   - **Младший аналитик**.
   - **Доступ к общим панелям мониторинга**. Роль доступна только при выборе тенанта Shared в раскрывающемся списке **Тенант**. Для тенанта Shared это единственная роль, которую можно добавить через параметры доменной аутентификации.

   После того как вы выберете роли, для каждой роли появится поле фильтра для группы. Укажите полный путь к группе домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для каждой роли. Пример ввода группы: `CN=KUMA team`, `OU=Groups`, `OU=Clients`, `DC=test`, `DC=domain`.

   Для каждого тенанта можно задать отдельный набор фильтров для ролей.

   Если для какой-то из ролей не указан фильтр, это означает что для данной роли не указаны условия создания учетной записи через доменную аутентификацию. Выполнить аутентификацию с такой ролью невозможно.

   После первой аутентификации пользователей под доменной учетной записью в разделе **Параметры** → **Доступ** → **Пользователи** будут созданы карточки доменных пользователей. Для доменного пользователя в карточке пользователя заблокирована возможность изменения основных ролей (Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик) и доступно добавление и удаление дополнительных ролей (Доступ к КИИ, Работа с НКЦКИ, Чтение общих ресурсов), включая управление привязкой дополнительных ролей к тенантам. Роли назначенные в разделе Доменной аутентификации и назначенные в карточке пользователя дополняют друг друга. Для Главного администратора дополнительные роли в KUMA активированы автоматически, поэтому не нужно добавлять их отдельно. Если доменному пользователю была присвоена роль Главного администратора, а затем роль Главного администратора отозвана, дополнительные роли нужно будет заново присвоить в карточке пользователя в разделе **Параметры** → **Доступ** → **Пользователи**.

   > Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, для каждой группы требуется повторить шаги 2–4, указывая при этом тот же тенант.

5. Если требуется, повторите шаги 2–4 для каждого тенанта, для которого вы хотите настроить доменную аутентификацию с ролями Младший аналитик, Аналитик первого уровня, Аналитик второго уровня или Администратор тенанта.

6. Нажмите на кнопку **Добавить**.

Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Доступ** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка подключения на стороне Active Directory Federation Services

В этом разделе приведены инструкции по созданию новой группы подключения и настройке правил для созданной группы подключения на стороне Active Directory Federation Services (AD FS).

На сервере должна быть уже настроена роль AD FS.

Создание новой группы подключения

1. В **Server Manager** в меню **Tools** выберите **ADFS Management**.

   В ADFS выберите раздел **Application groups** и в разделе **Actions** нажмите **Add Application Group**.

2. В открывшемся окне **Add Application Group Wizard** в разделе **Welcome** в поле **Name** укажите имя новой группы подключения. Пример: new-application-group.

   В поле **Template** в группе **Client-Server applications** выберите пункт **Native application accessing a web API**.

   Чтобы перейти к следующему этапу создания и настройки группы подключения, нажмите **Next**.

3. В открывшемся разделе **Native application** поля **Name** и **Client Identifier** заполняются автоматически.

   Значение поля **Client Identifier** понадобится указать в KUMA в поле **Client Identifier** при настройке доменной аутентификации.

   В поле **Redirect URI** введите URI для перенаправления из AD FS с обязательным указанием подстроки `/sso-callback` и нажмите **Add**. Пример: `https://adfs.example.com:7220/sso-callback`.

   Чтобы перейти к следующему этапу настройки, нажмите **Next**.

4. В открывшемся разделе **Configure Web API** в поле **Identifiers** добавьте идентификатор доверенной стороны и нажмите **Add**. Значение может быть любым. Пример: `test-demo`.

   Значение поля **Identifier** понадобится указать в KUMA в поле **Relying party identifiers** при настройке доменной аутентификации.

   Чтобы перейти к следующему этапу настройки, нажмите **Next**.

5. В открывшемся разделе **Apply Access Control Policy** выберите значение политики **Permit everyone**.

   Чтобы перейти к следующему этапу настройки, нажмите **Next**.

6. В открывшемся разделе **Configure Application Permissions** поле **Client application** заполняется автоматически.

В поле **Permitted scopes** установите флажок для параметров **allatclaims** и **openid**.

Чтобы перейти к следующему этапу настройки, нажмите **Next**.

7. В открывшемся разделе **Summary** проверьте настройки.

   Если настройки верны и вы готовы добавить группу, нажмите **Next**.

Новая группа будет добавлена. Вы можете перейти к настройке правил для созданной группы.

Добавление правил для группы подключения

1. В **Server Manager** в меню **Tools** выберите **ADFS Management**.

   В AD FS выберите раздел **Application groups** и в открывшемся окне выберите из списка необходимую группу подключения. Пример: `new-application-group`.

2. В окне **Application groups** в разделе **Actions** нажмите **Properties**.

   В открывшемся окне **new-application-group Properties** в разделе **Applications** выберите двойным нажатием **new-application-group - Web API**.

   В открывшемся окне **new-application-group - Web API Properties** перейдите на вкладку **Issuance Transform Rules** и нажмите **Add rule**.

   В открывшемся окне **Add Transform Claim Rule Wizard** в разделе **Choose Rule Type** выберите в раскрывающемся списке **Send LDAP Attributes as Claims**.

   Чтобы перейти к следующему этапу настройки, нажмите **Next**.

3. В разделе **Configure Claim Rule** в поле **Claim rule name** укажите имя правила. Пример: `rule-name-01`.

   В раскрывающемся списке **Attribute store** выберите **Active directory**.

   В поле **Mapping of LDAP attributes to outgoing claim types** сопоставьте следующие поля:

LDAP Attribute	Outgoing Claim Type
`User-Principal-Name`	`userPrincipalName`
`Display-Name`	`displayName`
`E-Mail-Addresses`	`mail`
`Is-Member-Of-DL`	`MemberOf`

   Чтобы завершить настройку, нажмите **Finish**.

4. Вернитесь к окну **new-application-group – Web API Properties** перейдите на вкладку **Issuance Transform Rules** и нажмите **Add rule**. В открывшемся окне **Add Transform Claim Rule Wizard** в разделе **Choose Rule Type** выберите в раскрывающемся списке **Send claims using a custom rule**.

   Чтобы продолжить настройку, нажмите **Next**.

5. В разделе **Configure Claim Rule** в поле **Claims rule name** укажите имя правила. Пример: `rule-name-02`.

   В поле **Custom rule** укажите следующие параметры:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]=> issue(store = "Active Directory", types = ("ObjectGUID"), query = ";ObjectGUID;{0}", param =
c.Value);
```

   Чтобы завершить настройку, нажмите **Finish**.

6. Система перейдет к окну **new-application-group – Web API Properties** и вкладке **Issuance Transform Rules**.

   Чтобы применить правила, на открывшейся вкладке **Issuance Transform Rules** нажмите **Apply** или **OK**.

Настройка групп и правил в AD FS завершена. Вы можете переходить к настройке доменной аутентификации в KUMA.

Устранение ошибки Access denied при входе в KUMA через ADFS

При попытке входа в KUMA через ADFS может появляться всплывающее сообщение `Access denied` или `Недостаточно прав`. В журнале ядра KUMA будет отображаться ошибка `Data source certificate has been changed`.

Эта ошибка свидетельствует о том, что изменился сертификат ADFS. Чтобы исправить ошибку и возобновить доменную аутентификацию, следует в настройках соединения с контроллером домена нажать на кнопку **Сбросить сертификат**. Новый сертификат будет сформирован автоматически.

Интеграция с НКЦКИ

Вы можете создать в веб-интерфейсе KUMA подключение к Национальному координационному центру по компьютерным инцидентам (далее "НКЦКИ"). Это позволит вам экспортировать в него инциденты, зарегистрированные в KUMA. Интеграция настраивается в разделе **Параметры** → **НКЦКИ** веб-интерфейса KUMA. Все поля, которые вы заполняете в настройках, автоматически будут отправляться в форму отправки данных в НКЦКИ.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Чтобы создать подключение к НКЦКИ:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Интеграции** → **НКЦКИ**.

2. С помощью переключателя **Состояние** включите интеграцию. По умолчанию интеграция выключена.

3. В поле **URL** введите URL, по которому доступен НКЦКИ.

4. В раскрывающемся списке **Тенант** выберите тенанта для сообщений от НКЦКИ.

5. В раскрывающемся списке **Токен** создайте или выберите существующий секрет с API-токеном, который был выдан вашей организации для подключения к НКЦКИ:

   - Если у вас уже есть секрет, его можно выбрать в раскрывающемся списке.

   - Если вы хотите создать новый секрет:

     a. Нажмите **Создать** и в окне **Создание секрета** укажите следующие параметры:

     - **Название** (обязательно) – уникальное имя создаваемого ресурса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

     - **Токен** (обязательно) – токен, который был выдан вашей организации для подключения к НКЦКИ.

     - **Описание** – описание сервиса: до 256 символов в кодировке Unicode.

b. При необходимости в раскрывающемся списке **Теги** выберите теги для интеграции.

c. Нажмите **Создать**.

Секрет с токеном для подключения к НКЦКИ создан. Он хранится в разделе **Ресурсы** → **Ресурсы** → **Секреты** и принадлежит главному тенанту.

6. В раскрывающемся списке **Сфера деятельности компании** выберите нужное значение.

7. В поле **Название компании** укажите название компании, для которой выполняется интеграция.

8. В раскрывающемся списке **Местоположение** укажите местоположение вашей компании.

9. В раскрывающемся списке **Корневой CA** создайте или выберите существующий секрет:

- Если у вас уже есть секрет, его можно выбрать в раскрывающемся списке.

- Если вы хотите создать новый секрет:

  a. Нажмите **Создать** и укажите следующие параметры:

  - **Название** – уникальное имя создаваемого ресурса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

  - **Тип** – тип секрета (сертификат).

  - **Файл сертификата** – нажмите кнопку **Загрузить сертификат** и выберите сертификат промежуточного удостоверяющего центра, скачанный и установленный на сервере Ядра KUMA.

    Скачать и установить сертификат промежуточного удостоверяющего центра.

    Чтобы установить и сделать доверенным сертификат промежуточного удостоверяющего центра на сервере Ядра KUMA:

    1. Перейдите по ссылке личного кабинета в НКЦКИ. Например, https://lk.cert.gov.ru.

    2. Правой кнопкой мыши вызовите контекстное меню **View site details** слева от ссылки в адресной строке.

       - Если вы используете защищенное соединение, в открывшемся контекстном меню выберите пункт **Connection is secure** и раскрывшемся списке в пункте **Certificate is valid** нажмите кнопку перехода **Show certificate**.

       - Если вы используете незащищенное соединение, в открывшемся меню нажмите **Certificate details**.

       В зависимости от браузера расположение меню и порядок пунктов могут отличаться.

    3. В открывшемся окне **Certificate Viewer** в блоке **Issued By** в поле **Common Name (CN)** указано имя нужного сертификата. Например, GlobalSign GCC R6 AlphaSSL CA 2023.

       Запомните имя сертификата, его необходимо будет скачать в следующем шаге.

    4. Перейдите по ссылке https://support.globalsign.com/ca-certificates/intermediate-certificates/alphassl-intermediate-certificates, найдите сертификат из шага 3 и нажмите View as BASE64.

5. Скопируйте отобразившиеся на экране строки сертификата в файл и добавьте файл со строчками сертификата в качестве секрета в KUMA.

6. После установки сертификата перезапустите сервер Ядра KUMA.

В результате сертификат установлен и вы можете продолжить настройку интеграции.

- **Теги** – теги для маркировки сертификата.

- **Описание** – описание сервиса: до 256 символов в кодировке Unicode.

b. Нажмите **Создать**.

Секрет с сертификатом промежуточного удостоверяющего центра создан. Он хранится в разделе **Ресурсы** → **Ресурсы** → **Секреты** и принадлежит главному тенанту.

10. При необходимости в блоке параметров **Прокси-сервер** создайте или выберите существующий прокси-сервер, который должен использоваться при подключении к НКЦКИ.

11. Укажите время ожидания ответа от НКЦКИ в секундах.

12. При необходимости укажите ИНН, адрес оператора и адрес электронной почты для отправки информации об уведомлении.

13. Нажмите **Сохранить**.

KUMA интегрирована с НКЦКИ. Теперь вы можете экспортировать в него инциденты. Вы можете нажать на кнопку **Проверить подключение**, чтобы убедиться, что с НКЦКИ устанавливается соединение.

Интеграцию можно включить или выключить с помощью флажка **Выключено**.

Возможные ошибки

Если при настройке интеграции с НКЦКИ возвращается ошибка *https://lk.cert.gov.ru/api/v2/incidents? x509: certificate signed by unknown authority,* **скачайте и установите сертификат промежуточного удостоверяющего центра на сервер Ядра KUMA**.

Чтобы установить и сделать доверенным сертификат промежуточного удостоверяющего центра на сервере Ядра KUMA:

1. Перейдите по ссылке личного кабинета в НКЦКИ. Например, https://lk.cert.gov.ru.

2. Правой кнопкой мыши вызовите контекстное меню **View site details** слева от ссылки в адресной строке.

   - Если вы используете защищенное соединение, в открывшемся контекстном меню выберите пункт **Connection is secure** и раскрывшемся списке в пункте **Certificate is valid** нажмите кнопку перехода **Show certificate**.

   - Если вы используете незащищенное соединение, в открывшемся меню нажмите **Certificate details**.

   В зависимости от браузера расположение меню и порядок пунктов могут отличаться.

3. В открывшемся окне **Certificate Viewer** в блоке **Issued By** в поле **Common Name (CN)** указано имя нужного сертификата. Например, GlobalSign GCC R6 AlphaSSL CA 2023.

   Запомните имя сертификата, его необходимо будет скачать в следующем шаге.

4. Перейдите по ссылке https://support.globalsign.com/ca-certificates/intermediate-certificates/alphassl-intermediate-certificates, найдите сертификат из шага 3 и нажмите View as BASE64.

5. Скопируйте отобразившиеся на экране строки сертификата в файл и добавьте файл со строчками сертификата в качестве секрета в KUMA.

6. После установки сертификата перезапустите сервер Ядра KUMA.

В результате сертификат установлен и вы можете продолжить настройку интеграции.

Интеграция с Security Orchestration Automation and Response Platform (SOAR)

Security Orchestration Automation and Response Platform (далее SOAR) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

SOAR можно интегрировать с KUMA. После настройки интеграции в SOAR можно выполнять следующие задачи:

- Запрашивать из KUMA сведения об алертах. При этом в SOAR по полученным данным создаются *инциденты*.

- Отправлять в KUMA запросы на закрытие алертов.

Интеграция реализована с помощью KUMA REST API. На стороне Security Vision IRP интеграция осуществляется с помощью преднастроенного коннектора **Kaspersky KUMA**. О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика SOAR.

Работа с инцидентами SOAR

Инциденты SOAR, созданные на основе данных об алертах KUMA, можно просмотреть в SOAR в разделе **Инциденты** → **Инциденты (2 линии)** → **Все инциденты (2 линии)**. В каждый инцидент SOAR записываются события, относящиеся к алертам KUMA. Импортированные события можно просмотреть на вкладке **Реагирование**.

Алерт KUMA, импортированный в SOAR в качестве инцидента

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Id: 1781339 Тип: Инцидент (2 линии)

Дата и время создания: 16:06:07 14.04.2022

Доступные базовые действия:

Взять в работу

Доступные действия по реагированию:

Общая информация

Наименование: Обнаружен инцидент Test Correlation rule у Main

Описание: Обнаружен алерт [redacted] вида "Test Correlation rule" на инфраструктуре Main в 13:05:56 14.04.2022. Адрес источника - [redacted], Адрес назначения - [redacted]

Информация об источнике

IP-адрес источника: [redacted]

Порт источника: [redacted]

Имя узла источника:

Имя пользователя:

Активы источника

Информация о назначении

IP-адрес назначения: [redacted]

Порт назначения:

Имя узла назначения: [redacted]

Имя пользователя назначения:

Активы назначения

Обработка инцидента

Приоритет: Низкий

Группа исполнения: Мониторинг инцидентов КБ

Исполнитель:

Этап обработки: Ожидание взятия в работу

Статус: Новый

Ложное срабатывание:

Вердикт:

Рекомендации:

Обработка инцидента(SLA)

Дата и время создания: 16:06:07 14.04.2022

Дата и время взятия в работу:

Дата и время закрытия:

Сохранить | Сохранить и выйти | Отмена

Инцидент в Security Vision IRP, созданный на основе алерта KUMA

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Jira

Идентификатор Jira:

Статус Jira:

Переписка с пользователем

Почтовая переписка:

Вложения почтовой переписки:

Обогащение из AD

Информация о пользователе из AD:

Координата X:

Координата Y:

События QRadar

Событие	Время события	Имя пользователя	IP-адрес источника	Порт источника	IP-адрес назначения
service started	2022-04-14T16:05:51.000+03:00		[redacted]	[redacted]	[redacted]
service started	2022-04-14T16:05:56.000+03:00		[redacted]	[redacted]	[redacted]

События из алерта KUMA, импортированные в Security Vision IRP

Настройка интеграции в KUMA

Для того чтобы настроить интеграцию KUMA и SOAR необходимо настроить авторизацию API-запросов в KUMA. Для этого требуется создать токен для пользователя KUMA, от имени которого будут обрабатываться API-запросы на стороне KUMA.

Токен можно сгенерировать в профиле своей учетной записи. Пользователи с ролью главный администратор могут генерировать токены в учетных записях других пользователей. Вы всегда можете сгенерировать новый токен.

Чтобы сгенерировать токен в профиле своей учетной записи:

1. В веб-интерфейсе KUMA в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.

2. Нажмите на кнопку **Сгенерировать токен**.

3. В открывшемся окне скопируйте созданный токен. Он потребуется для настройки SOAR.

   При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

Сгенерированный токен требуется указать в параметрах коннектора SOAR.

Настройка интеграции в SOAR

Настройка интеграции в SOAR заключается в импорте и настройке коннектора. При необходимости можно также изменить другие параметры SOAR, связанные с обработкой данных KUMA: например, расписание обработки данных и рабочий процесс.

Более подробные сведения о настройке SOAR см. в документации продукта.

Импорт и настройка коннектора

Добавление коннектора в SOAR

Интеграция SOAR и KUMA осуществляется с помощью коннектора **Kaspersky KUMA**. О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика SOAR.

*Чтобы импортировать коннектор **Kaspersky KUMA** в SOAR:*

1. В SOAR откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в SOAR.

2. В верхней части экрана нажмите на кнопку импорта и выберите zip-архив с коннектором **Kaspersky KUMA**.

Коннектор импортирован в SOAR и готов к настройке.

Настройка в коннекторе подключения к KUMA

Для использования коннектора нужно настроить его подключение к KUMA.

*Чтобы настроить в SOAR подключение к KUMA с помощью коннектора **Kaspersky KUMA**:*

1. В SOAR откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в вашу SOAR.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие параметры коннектора.

3. В разделе **Параметры коннектора** нажмите на кнопку **Редактировать**.

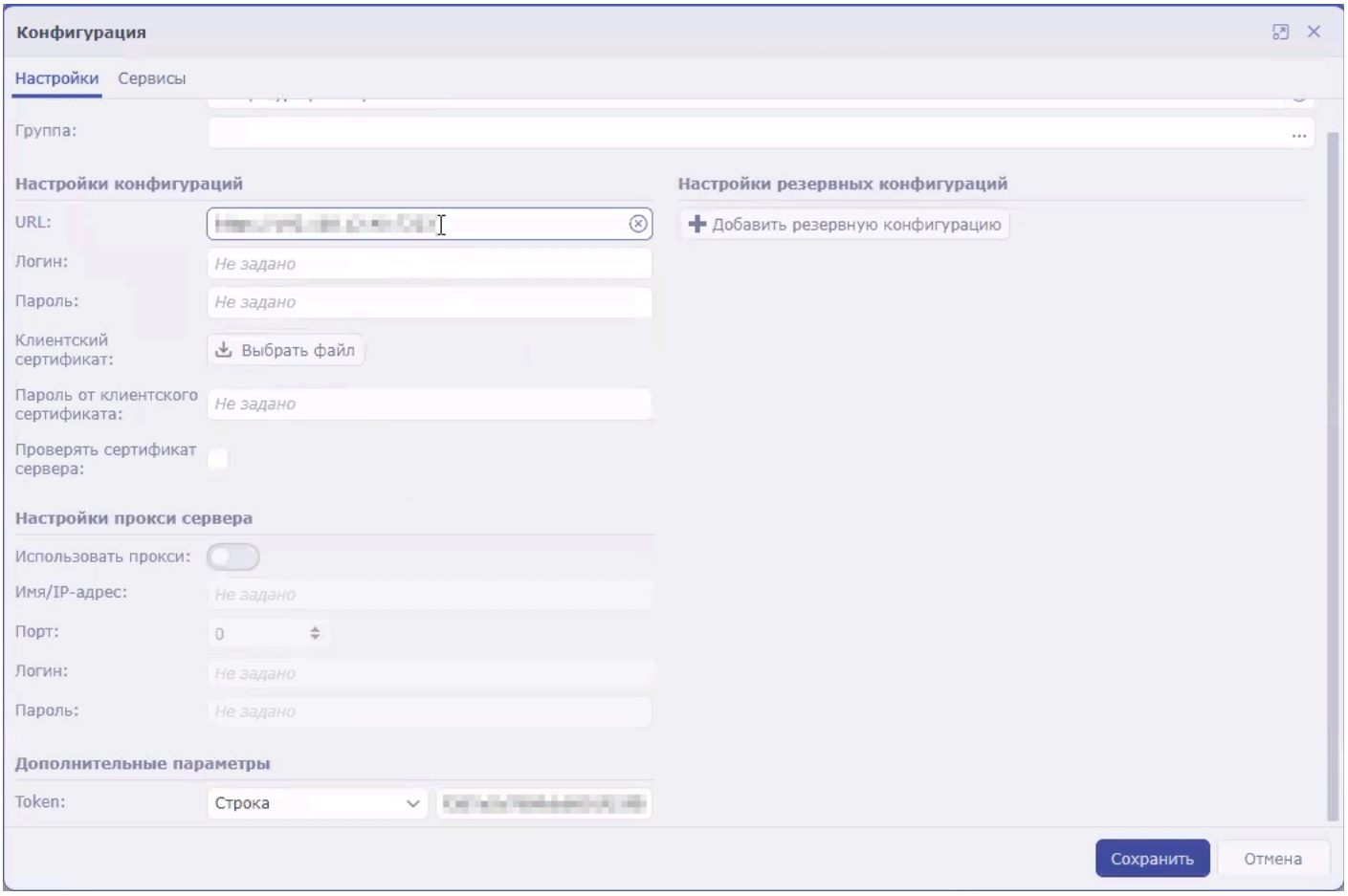
   Отобразится конфигурация коннектора.

4. В поле **URL** укажите адрес и порт KUMA. Например, `kuma.example.com:7223`.

5. В поле **Token** укажите API-токен пользователя KUMA.

Подключение к KUMA настроено в коннекторе SOAR (см. рисунок по ссылке ниже).

Настройки коннектора Security Vision IRP



Настройки коннектора Security Vision IRP

Настройка в коннекторе SOAR команд для взаимодействия с KUMA

С помощью SOAR можно получать сведения об алертах KUMA (или *инцидентах* в терминологии SOAR), а также отправлять запросы на их закрытие. Для выполнения этих действий в коннекторе SOAR нужно настроить соответствующие команды.

В инструкциях ниже описано, как добавить команды на получение и закрытие алертов, однако при необходимости реализовать более сложную логику взаимодействия SOAR и KUMA вы можете аналогичным образом создать команды с другими API-запросами.

Чтобы настроить команду на получение из KUMA сведений об алертах:

1. В SOAR откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в SOAR.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.

3. Нажмите на кнопку **+Команда**.

   Откроется окно создания команды.

4. Укажите параметры команды для получения алертов:

   - В поле **Наименование** введите название команды: `Получение инцидентов`.
   - В раскрывающемся списке **Тип запроса** выберите **GET**.
   - В поле **Вызываемый метод** введите API-запрос на поиск алертов:

     `api/v1/alerts/?withEvents&status=new`

   - В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
   - В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

Команда коннектора настроена. При этой команды коннектор SOAR будет запрашивать в KUMA сведения обо всех алертах со статусом **Новый** и всех относящихся к ним событиях. Полученные данные будут передаваться в обработчик SOAR, который на их основе будет создавать инциденты SOAR. Если алерт уже был импортирован в SOAR, но в нем появились новые данные, сведения о нем будут обновлены в SOAR.

Чтобы настроить команду на закрытие алертов KUMA:

1. В SOAR откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в SOAR.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.

3. Нажмите на кнопку **+Команда**.

   Отобразится окно создания команды.

4. Укажите параметры команды для получения алертов:

- В поле **Наименование** введите название команды: `Закрытие инцидента`.
- В раскрывающемся списке **Тип запроса** выберите **POST**.
- В поле **Вызываемый метод** введите API-запрос на закрытие алерта:

  `api/v1/alerts/close`
- В поле **Запрос** введите содержимое отправляемого API-запроса:

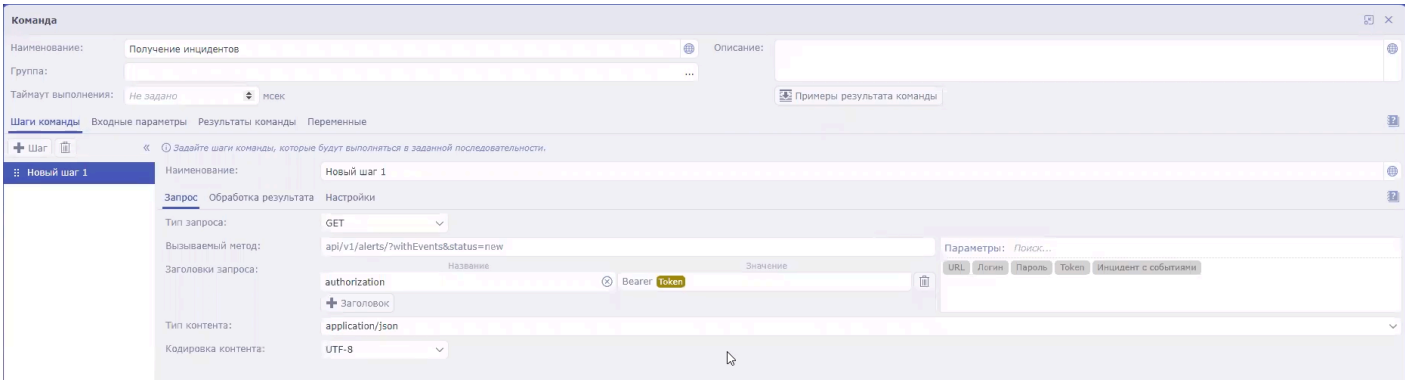
  `{"id":"<Идентификатор алерта>","reason":"responded"}`

  Можно создать несколько команд для разных причин закрытия алертов: responded, incorrect data, incorrect correlation rule.
- В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
- В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

Команда коннектора настроена (см. рисунок по ссылке ниже). При выполнении этой команды в SOAR будет закрыт инцидент, а в KUMA будет закрыт соответствующий ему алерт.

Создание команд в SOAR



Создание команд в SOAR

После настройки коннектора SOAR алерты KUMA будут поступать в платформу в виде инцидентов SOAR. Далее необходимо настроить обработку инцидентов в SOAR в соответствии с существующей в вашей организации политикой безопасности.

Настройка обработчика, расписания и рабочего процесса

Обработчик SOAR

Обработчик SOAR принимает от коннектора SOAR данные об алертах KUMA и создает на их основе инциденты SOAR. Для обработки используется предустановленный обработчик **KUMA (Инциденты)**. Настройки обработчика **KUMA (Инциденты)** доступны в SOAR в разделе **Настройки** → **Обработка событий** → **Обработчики событий**:

- Правила обработки алертов KUMA можно просмотреть в настройках обработчика на вкладке **Нормализация**.
- Действия при создании новых объектов можно просмотреть в настройках обработчика на вкладке **Действия** для создания объектов типа **Инцидент (2 линии)**.

Расписание запуска обработчика

Запуск коннектора и обработчика выполняется по предустановленному расписанию **KUMA**. Настройка этого расписания доступна в SOAR в разделе **Настройки** → **Обработка событий** → **Расписание**:

- В блоке параметров **Настройки коннектора** можно настроить параметры запуска коннектора.
- В блоке параметров **Настройки обработки** можно настроить параметры запуска обработчика.

Рабочий процесс SOAR

Жизненный цикл инцидентов SOAR, созданных на основе алертов KUMA, проходит по преднастроенному процессу **Обработка инц. (2 линии)**. Настройка рабочего процесса доступна в SOAR в разделе **Настройки** → **Рабочие процессы** → **Шаблоны рабочих процессов**: выберите процесс **Обработка инц. (2 линии)** и нажмите на транзакцию или состояние, которое необходимо изменить.

Интеграция с KICS for Networks и KATA

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. Программа анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

Kaspersky Anti Targeted Attack (далее KATA) – приложение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки (англ. advanced persistent threats).

KICS for Networks или KATA можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Импортировать из KICS for Networks или KATA в KUMA сведения об активах.

  Импорт информации об активах из KATA версии 7.1 доступен только для KUMA версии 4.0 и выше.

- Отправлять из KUMA в KICS for Networks или KATA команды на изменение статусов активов.

В отличие от KUMA, в KICS for Networks и KATA активы называются устройствами.

Интеграцию KICS for Networks или KATA и KUMA необходимо настроить с обеих сторон:

1. В KICS for Networks или KATA нужно создать коннектор KUMA и сохранить файл свертки этого коннектора.

   Интеграцию можно настроить как на стороне KICS for Networks версии 4.0 и выше, так и на стороне KATA версии 7.0 и выше. Настройка интеграции с любой стороны позволяет правильно передавать сведения об активах и события в KUMA.

2. В KUMA с помощью файла свертки коннектора нужно создать подключение к KICS for Networks или KATA.

Описываемая в этом разделе интеграция касается импорта сведений об активах. KICS for Networks или KATA можно также настроить на отправку событий в KUMA. Для этого необходимо в KICS for Networks или KATA создать коннектор типа SIEM/Syslog, а на стороне KUMA – настроить коллектор.

Настройка интеграции в KICS for Networks и KATA

Настройку интеграции можно выполнить на стороне KICS for Networks версии 4.0 или на стороне KATA версии 7.0 и выше. Для правильной работы импорта данных и событий необходимо использовать коннектор KUMA и файл свертки, созданный в соответствующей системе.

Настройку интеграции KICS for Networks или KATA и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

На стороне KICS for Networks или KATA настройка интеграции заключается в создании *коннектора типа KUMA*. В KICS for Networks и KATA коннекторы – это специальные программные модули, которые обеспечивают обмен данными KICS for Networks и KATA со сторонними системами, в том числе с KUMA. Подробнее о создании коннекторов см. в документации KICS for Networks.

При добавлении в KICS for Networks или KATA коннектора автоматически создается *файл свертки* для этого коннектора. Файл свертки – это зашифрованный файл конфигурации для подключения к KICS for Networks или KATA, который используется при настройке интеграции на стороне KUMA.

Настройка интеграции в KUMA

Настройку интеграции KICS for Networks или KATA 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 или KATA:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **KICS/KATA**.

   Откроется окно **Интеграция с KICS/KATA по тенантам**.

2. Нажмите на кнопку **Добавить параметры для нового тенанта**.

3. В открывшемся окне настройте следующие параметры интеграции с KICS for Networks или KATA:

   - Включите переключатель **Состояние**. По умолчанию переключатель включен.
   - В раскрывающемся списке **Тенант** выберите тенант для интеграции с KICS for Networks или KATA.
   - Включите переключатель **Включить реагирование**, чтобы иметь возможность изменять статусы активов KICS for Networks или KATA с помощью правил реагирования KUMA.

4. В блоке с таблицей **Подключения** добавьте новое подключение, нажав на кнопку **+ Добавить**.

5. В открывшемся окне **Создать подключение** настройте следующие параметры:

   - Включите переключатель **Состояние**. По умолчанию переключатель включен.
   - В поле **Файл свертки** нажмите на значок добавления (+) и выберите файл свертки коннектора, созданный в KICS for Networks или KATA при создании коннектора для подключения к KUMA.
   - В поле **Пароль файла свертки** введите пароль, заданный для файла свертки.
   - В поле **Версия API** укажите версию API, используемую в KICS for Networks или KATA. Значение по умолчанию: `Авто` (версия 4.0).

6. Нажмите **Сохранить**.

   Созданное подключение автоматически отобразится в таблице подключений выбранного тенанта.

7. При необходимости добавьте еще несколько подключений в рамках одного тенанта.

8. В окне **Интеграция с KICS/KATA по тенантам** нажмите **Добавить**.

В KUMA будет настроена интеграция с KICS for Networks или KATA. Вы можете просмотреть идентификатор узла, на котором будет работать коннектор KICS for Networks или KATA, перейдя по ссылке с его IP-адресом.

Включение и выключение интеграции с KICS for Networks или KATA

Чтобы включить или выключить для тенанта интеграцию с KICS for Networks или KATA:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **KICS/KATA**.

   Откроется окно **Интеграция с KICS/KATA по тенантам**.

2. Выполните одно из следующих действий:

   - С помощью переключателя **Состояние** включите или выключите интеграцию для интересующего вас тенанта.
   - Нажмите на кнопку **Добавить параметры для нового тенанта** и в открывшемся окне с помощью переключателя **Состояние** включите или выключите интеграцию для интересующего вас тенанта, после чего сохраните внесенные изменения.

Изменение частоты обновления данных

KUMA обращается к KICS for Networks или KATA 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 или KATA создается задача в разделе **Диспетчер задач** веб-интерфейса KUMA.

Чтобы изменить расписание импорта сведений об активах KICS for Networks или KATA:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **KICS/KATA**.
2. Выберите нужный тенант.

   Откроется окно **Интеграция с KICS/KATA по тенантам**.
3. В поле **Интервал обновления в часах** укажите требуемую частоту обновления данных в часах. Значение по умолчанию – 3.
4. Сохраните изменения.

Расписание импорта изменено.

Особенности импорта информации об активах из KICS for Networks и KATA

Независимо от того, с какой стороны инициирована интеграция (KICS for Networks или KATA), импорт активов и уязвимостей в KUMA выполняется по стандартным правилам и с сохранением идентификаторов.

Импорт активов

Активы импортируются в соответствии с правилами импорта активов. Импортируются только активы со статусами **Разрешенное** и **Неразрешенное**.

Активы KICS for Networks и KATA идентифицируются по комбинации следующих параметров:

- IP-адрес экземпляра KICS for Networks или KATA, с которым настроена интеграция.
- Идентификатор коннектора KICS for Networks или KATA, с помощью которого настроена интеграция.
- Идентификатор, присвоенный активу (или "устройству") в экземпляре KICS for Networks или KATA.

Импорт сведений об уязвимостях

При импорте активов в KUMA также поступают сведения об активных уязвимостях KICS for Networks и KATA. Если в KICS for Networks или KATA уязвимость была отмечена 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 или KATA.

> В KICS for Networks и KATA 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 или KATA, актив удаляется по прошествии 30 дней.

Изменение статуса актива KICS for Networks и KATA

После настройки интеграции вы можете менять статусы активов KICS for Networks или KATA из KUMA. Статусы можно менять автоматически и вручную.

Статусы активов можно менять, только если вы включили реагирование в настройках подключения к KICS for Networks или KATA.

Изменение статуса актива KICS for Networks или KATA вручную

Пользователи с ролями Главный Администратор, Администратор тенанта и Аналитик второго уровня в доступных им тенантах могут вручную менять статусы активов, импортированных из KICS for Networks или KATA.

Чтобы вручную изменить статус актива KICS for Networks или KATA:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.

2. В раскрывающемся списке **Статус KICS/KATA** выберите статус, который необходимо присвоить активу KICS for Networks или KATA. Доступны статусы *Разрешенное* или *Неразрешенное*.

Статус актива будет изменен. Новый статус отобразится в KICS for Networks или KATA и в KUMA.

Изменение статуса актива KICS for Networks или KATA автоматически

Автоматическое изменение статусов активов KICS for Networks или KATA реализовано с помощью правил реагирования. Правила необходимо добавить в коррелятор, который будет определять условия их срабатывания.

Интеграция с Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также "ASAP") – 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 ASAP можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Менять группы обучения пользователей.
- Просматривать информацию пользователей о пройденных курсах и полученных сертификатах.

Интеграция ASAP и KUMA заключается в настройте API-подключения к платформе ASAP. Процесс происходит в обоих продуктах:

1. В ASAP необходимо создать токен для авторизации API-запросов и получить адрес для API-запросов.
2. В KUMA необходимо указать адрес для API-запросов в ASAP, добавить токен для авторизации API-запросов, а также указать адрес электронной почты администратора ASAP для получения уведомлений.

Создание токена в ASAP и получение ссылки для API-запросов

Для авторизации API-запросов из KUMA в ASAP их необходимо подписывать токеном, созданном в платформе ASAP. Только администраторы компании могут создать токены.

Создание токена

Чтобы создать токен:

1. Войдите в веб-интерфейс платформы ASAP.
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 для вас способом: этот токен потребуется указать при настройке интеграции в KUMA.

> Токен не хранится в системе ASAP 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.

Выпущенный токен действителен в течение 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 ASAP для API-запросов:

1. Войдите в веб-интерфейс платформы ASAP.

2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.

3. Ссылка для обращения к ASAP через Open API расположена в нижней части окна. Скопируйте ее и сохраните любым удобным для вас способом: эту ссылку потребуется указать при настройке интеграции в KUMA.

Настройка интеграции в KUMA

Чтобы настроить в KUMA интеграцию с ASAP:

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Интеграции** → **Kaspersky Automated Security Awareness Platform**.

   Откроется окно **Интеграция с Kaspersky Automated Security Awareness Platform**.

2. Убедитесь, что переключатель **Состояние** включен и интеграция активирована.

3. В раскрывающемся списке **Секрет** выберите секрет для использования в интеграции с Kaspersky Automated Security Awareness Platform. При необходимости вы также можете создать секрет типа **token**, указав в нем токен, полученный в платформе ASAP. Для этого выполните следующие действия:

   a. В раскрывающемся списке **Секрет** нажмите **Создать**.

      Откроется окно **Создание секрета**.

   b. В поле **Название** введите название для секрета. Должно содержать от 1 до 128 символов в кодировке Unicode.

   c. В поле **Токен** введите токен для авторизации API-запросов в ASAP.

   d. При необходимости в раскрывающемся списке **Теги** выберите теги для секрета.

   e. При необходимости добавьте описание секрета в поле **Описание**.

   f. Нажмите **Создать**.

4. В поле **URL для OpenAPI ASAP** укажите адрес, используемый платформой ASAP для API-запросов.

5. В поле **Адрес электронной почты администратора ASAP** укажите адрес электронной почты администратора ASAP, который должен получать уведомления при добавлении пользователей в группы обучения через KUMA.

6. В раскрывающемся списке **Шаблон уведомлений** выберите шаблон, который KUMA будет использовать для направления уведомлений. При необходимости вы также можете создать шаблон уведомления, нажав **Создать**.

7. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера выберите, который следует использовать для подключения к платформе ASAP.

8. Нажмите **Сохранить**.

В KUMA настроена интеграция с ASAP. 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 ASAP и изменение учебных групп

После настройки интеграции ASAP и KUMA в алертах и инцидентах при просмотре данных о связанных с ними пользователях становятся доступны данные из ASAP:

- Сведения об учебной группе, 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 ASAP:

1. В веб-интерфейсе KUMA 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 ASAP**.

В окне отображаются данные пользователя из ASAP.

Вы можете изменить учебную группу пользователя ASAP.

Чтобы изменить учебную группу ASAP:

1. В веб-интерфейсе KUMA 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 ASAP** выберите учебную группу ASAP, в которую вы хотите поместить пользователя.
4. Нажмите **Применить**.

Пользователь будет перемещен в выбранную группу ASAP, администратор компании платформы ASAP 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 ASAP.

Отправка уведомлений в Telegram

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Совместимость подтверждена только для версии KUMA 2.0 и выше.
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 настройки приватности:

   a. В чате бота BotFather введите команду:

   `/mybots`

   b. Выберите нужный бот из списка.

   c. Нажмите **Bot Settings** → **Group Privacy** и выберите опцию **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 веб-интерфейсе KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **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 **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

   a. В разделе **Ресурсы** → **Корреляторы** 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 сервисы**.

   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.
Совместимость подтверждена только для KUMA версии 2.0 и выше и UserGate версии 6.0 и выше.
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 **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 **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 **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 веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **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 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 веб-интерфейсе KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **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 **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

   a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, который будет выполнять реагирование и в папку 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 сервисов**.

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.
Совместимость подтверждена только для KUMA версии 2.0 и выше и Kaspersky Web Traffic Security версии 6.0 и выше.
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 веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **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. Чтобы получить скрипт и библиотеку, обратитесь к сотруднику технической поддержки.

3. Разместите полученный от сотрудника технической поддержки 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 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 веб-интерфейсе KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **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 **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, который будет выполнять реагирование и в папку 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 сервисов**.

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.
Совместимость подтверждена только для KUMA версии 2.0 и выше и Kaspersky Secure Mail Gateway версии 2.0 и выше.
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 веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **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. Чтобы получить скрипт и библиотеку, обратитесь к сотруднику технической поддержки.

3. Разместите полученный от сотрудника технической поддержки 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 команду:

   ```
   chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py
   ```

Скрипт будет готов к использованию.

Настройка правила реагирования для интеграции с KSMG

Чтобы настроить правило реагирования:

1. Создайте правило реагирования:

   a. В веб-интерфейсе KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **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. ksmg.py.

f. В поле **Аргументы скрипта** укажите:

- `--host` – адрес сервера KSMG.
- `--username` – имя учетной записи пользователя, созданной в KSMG.

  Вы можете указать учетную запись Administrator.
- `--password` – пароль учетной записи пользователя KSMG.
- `--rule_id` – ID правила, созданного в KSMG.
- Укажите один из ключей в соответствии с типом блокируемого объекта:
  - `--email` – укажите поле события KUMA, из которого вы хотите получать email, например `{{.SourceUserName}}`.
  - `--ip` – укажите поле события KUMA, из которого вы хотите получать IP-адрес, например `{{.SourceAddress}}`.
- `--ntlm` – укажите этот ключ, если пользователь KSMG был создан с NTLM-аутентификацией.

```
Пример:
 --host <address> --username <user> --password <pass> --ntlm --rule_id <id> --email {{.SourceUserName}}
```

g. В блоке **Условия** добавьте условия, соответствующие правилам корреляции, по срабатыванию которых необходима блокировка IP-адреса или адреса электронной почты отправителя сообщения в KSMG.

h. Нажмите **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, который будет выполнять реагирование и в папку 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 сервисов**.

g. Нажмите на кнопку **Сохранить**.

Правило реагирования будет привязано к коррелятору и готово к использованию.

Интеграция с Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (далее также MDR) представляет собой решение для автоматического обнаружения и анализа инцидентов безопасности в вашей инфраструктуре с помощью телеметрии и передовых технологий машинного обучения.

Вы можете настроить интеграцию KUMA с Kaspersky Managed Detection and Response, чтобы автоматически импортировать инциденты из Консоли MDR в KUMA для последующей обработки и анализа.

Для настройки интеграции вам нужно выполнить следующие действия:

1. Выполнить предварительную настройку.
2. Настроить интеграцию с MDR.

Предварительная настройка

Чтобы выполнить предварительную настройку:

1. Откройте доступ к Консоли MDR.

   Убедитесь, что на сервере, на котором будет настроена интеграция с KUMA, есть сетевой доступ к веб-адресу https://mdr.kaspersky.com по порту **TCP/443**.

2. В KUMA создайте пользователя с ролью Администратор тенанта.

   Убедитесь, что у этого пользователя есть доступ к API и возможность выполнять запросы POST /events.

3. В Консоли MDR сгенерируйте API-токен, выполнив следующие действия:

   a. В окне Консоли MDR выберите пункт меню **Параметры**.

   b. Перейдите на вкладку **API**.

   c. В верхней части окна нажмите на кнопку **Добавить**.

   d. Укажите следующие параметры:

   - **Название подключения**.

     Название подключения может содержать латинские буквы, цифры и специальные символы. Это название будет использоваться в качестве имени пользователя при создании инцидентов, комментариев и вложений, так как токен доступа не привязан к конкретному пользователю.

   - **Права доступа**.

     Выберите, какие права доступа необходимо предоставить для выполнения действий через HTTP API.

   - **Тенант**.

     При необходимости выберите одного или несколько тенантов.

Если для создаваемых в Консоли MDR инцидентов в раскрывающемся списке **Тенант** отсутствует значение, укажите значение **Корень без тенантов**, чтобы при подключении скрипт обнаружил эти инциденты.

e. В нижней части раздела нажмите на кнопку **Создать**. После этого отобразятся значения следующих параметров:

- **Токен JWT** (refresh_token) – токен, который используется для получения access_token, необходимого для авторизации при работе с API.
- **Идентификатор клиента** (client_id) – идентификатор, который необходимо передавать при запросах к API.

4. Скачайте архив kuma_mdr_integration.tar.gz со скриптом по следующей ссылке:

   https://box.kaspersky.com/f/11a58e42f63e4cef8741/

5. Настройте цепочку сертификатов для MDR, выполнив следующие действия:

   a. В браузере откройте ссылку https://mdr.kaspersky.com.

   b. Нажмите на значок замка в адресной строке рядом с веб-адресом сайта.

   c. Выберите пункт **Безопасное подключение** и нажмите **Действительный сертификат**.

   d. Перейдите на вкладку **Подробнее**.

   e. Для каждого элемента в иерархии сертификатов (начиная с нижнего ***.mdr.kaspersky.com** и заканчивая корневым **DigiCert Global Root G2**) нажмите на кнопку **Экспорт**.

   f. Добавьте сохраненные сертификаты в файл с расширением .PEM (например, mdr.pem). Сертификаты должны быть размещены в порядке от нижнего к корневому.

Инициализация интеграции

Чтобы настроить интеграцию KUMA с Kaspersky Managed Detection and Response:

1. Подготовьте файлы на сервере, выполнив следующие действия:

   a. Скопируйте архив kuma_mdr_integration.tar.gz на сервер KUMA (при распределенной установке – на сервер Core).

   b. Распакуйте архив в директорию /opt с помощью команды:

   ```
   sudo tar -xf kuma_mdr_integration.tar.gz -C /opt
   ```

2. Настройте конфигурационный файл, выполнив следующие действия:

   a. Перейдите в директорию /opt/mdr/conf и откройте на редактирование файл config.yml.

   b. В секции `General settings` укажите следующие параметры:

      - актуальный путь к директориям (по умолчанию указан /opt/mdr/*);
      - `client_id` (идентификатор клиента).

   c. В секции `Modules settings` → `kuma` укажите следующие параметры:

      - `api_url` – адрес API-интерфейса KUMA;
      - `username` – имя ранее добавленного пользователя с доступом к API;
      - `password` – пароль добавленного пользователя;
      - `tenantId` – идентификатор тенанта, в который будут импортироваться инциденты.

   d. В секции `Modules settings` → `logging` укажите актуальный путь к директории, где хранится скрипт (по умолчанию указан /opt/mdr/log).

3. Добавьте токен авторизации MDR, выполнив следующие действия:

   a. Перейдите в директорию /opt/mdr/conf, откройте на редактирование файл .refresh_token и вставьте в него ранее сгенерированный токен доступа к API MDR.

   b. Убедитесь, что в конце файла нет символа новой строки `\n`, так как это может привести к ошибке аутентификации. Для проверки вы можете выполнить следующие команды:

      ```
      # Проверка наличия символа новой строки
      wc -l /opt/mdr/conf/.refresh_token
      # Если выводится "1 .refresh_token", удалите символ
      perl -p -i -e 'chomp if eof' /opt/mdr/conf/.refresh_token
      # Повторная проверка
      wc -l /opt/mdr/conf/.refresh_token
      # Ожидаемый результат — "0 .refresh_token"
      ```

4. Укажите время начала сбора инцидентов, выполнив следующие действия:

   a. Перейдите в директорию /opt/mdr/conf и откройте на редактирование файл .last_check.

   b. В открывшемся файле укажите метку времени (в миллисекундах, 13 цифр), начиная с которого необходимо импортировать инциденты.

      Для того чтобы проверить, правильно ли вы выполнили настройку, рекомендуется указать время, предшествующее появлению последнего инцидента (например, `1672520400000`).

5. Обновите сертификат MDR. В директории /opt/mdr/conf/ замените файл mdr.pem на файл с актуальным сертификатом, который вы создали ранее.

6. Запустите скрипт интеграции main.py с помощью команды `python3 ./main.py`:

   - Если при первом запуске отображаются сообщения об отсутствии необходимых пакетов, установите их.

   - Если после запуска скрипта не отображаются сообщения об ошибках (кроме предупреждений о недействительном сертификате), интеграция настроена правильно.

   Журнал работы скрипта доступен по пути: /opt/mdr/log/app.log.

7. Проверьте импорт инцидентов.

   Убедитесь, что в KUMA были импортированы инциденты, созданные в Консоли MDR, начиная с момента времени, которое вы указали в файле .last_check.

8. Запустите скрипт в фоновом режиме, выполнив следующие действия:

   a. Остановите текущий сеанс запуска скрипта (если запущен).

   b. Повторно запустите скрипт main.py в фоновом режиме с помощью команды:

   ```
   nohup python3 /opt/mdr/main.py &
   ```

9. Настройте автозапуск скрипта после перезагрузки сервера, выполнив следующие команды:

   ```
   sudo crontab -e
   @reboot sleep 300 && python3 /opt/mdr/main.py &
   ```

   > Задержка в 5 минут (`sleep 300`) необходима для запуска службы kuma-core до запуска скрипта интеграции.

   Интеграция KUMA с Kaspersky Managed Detection and Response настроена. Теперь инциденты из Консоли MDR будут автоматически импортироваться в KUMA для последующей обработки и анализа.

Импорт информации об активах из RedCheck

> Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
> Совместимость подтверждена только для KUMA версии 2.0 и выше и RedCheck версии 2.6.8 и выше.
> 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 хостам.

Импортированные активы отображаются в веб-интерфейсе KUMA в разделе **Активы**. 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 тенанта или Аналитика второго уровня.
   - 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 kuma.example.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 будут отображаться 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	Обязательный	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 тенанта или Аналитика второго уровня.
`--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.
`--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 был пропущен хост с fqdn=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 разделе веб-интерфейса KUMA 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 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 сервис rsyslog.

Чтобы настроить передачу событий Sendmail в коллектор:

1. Подключитесь к серверу, на котором установлен Sendmail, под учетной записью с правами администратора.
2. В директории /etc/rsyslog.d/ создайте файл Sendmail-to-siem.conf и добавьте в него строку:

   ```
   If $programname contains 'sendmail' then @<collector_IP>:<collector_port>
   ```

   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 @@<collector IP>:<collector_port>
```

где:

- <collector_IP> — IP-адрес коллектора.
- <collector_port> — 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 сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Управление KUMA

В этом разделе описываются общие параметры KUMA.

Вход в веб-интерфейс решения

В веб-интерфейс KUMA могут входить только пользователи со статусом учетных записей *Активная*.

KUMA не позволяет создать для одного пользователя одновременно несколько сеансов. При попытке войти в веб-интерфейс KUMA повторно, например из другого браузера, первый сеанс автоматически завершится.

Рекомендуем настроить требования к паролям и правила входа в веб-интерфейс решения в политике безопасности.

Чтобы войти в веб-интерфейс решения:

1. В браузере введите следующий адрес:

   `https://<IP-адрес или FQDN сервера Ядра KUMA>:7220`

   Откроется страница авторизации веб-интерфейса с запросом на ввод логина и пароля учетной записи.
2. В поле **Логин** введите логин учетной записи.
3. В поле **Пароль** введите пароль указанной учетной записи.

Учетные данные для входа по умолчанию:

- Логин – admin
- Пароль – mustB3Ch@ng3d!

После первого входа измените пароль учетной записи admin.

4. Нажмите на кнопку **Войти**.

   Если вы ввели неверные учетные данные, KUMA сможет обработать следующую попытку входа через 3 секунды. Задержка по времени помогает предотвратить вход злоумышленника в веб-интерфейс KUMA с помощью перебора пароля. Если вы введете неверные учетные данные несколько раз подряд, ваша учетная запись будет заблокирована. Максимальное количество неудачных попыток входа и длительность блокировки учетной записи регулируются политикой безопасности.

Откроется главное окно веб-интерфейса решения.

В режиме мультитенантности при первом входе в веб-интерфейс решения пользователю отображаются данные только тех тенантов, которые были выбраны для него при создании его учетной записи.

Чтобы выйти из веб-интерфейса решения,

в левом нижнем углу веб-интерфейса KUMA нажмите на имя учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Выход**.

Настройка параметров Ядра KUMA

Чтобы настроить параметры Ядра KUMA:

1. Перейдите в раздел **Параметры** → **Другое** → **Общее** в веб-интерфейсе KUMA.
2. 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.

- 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.

3. 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.

4. 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 - 10000 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 решением: 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 решение 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 внутренних 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 проводит такие операции ежедневно. Вы можете указать значение от 0 до 23 включительно.

  > Мы рекомендуем проводить операции по самообслуживанию Ядра KUMA в ночное время, когда пользователи не используют функциональные возможности ядра.

  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-адрес балансировщика.

  URL-адрес балансировщика указывается в формате `hostname:port`, где:

  - `hostname` – имя хоста балансировщика;
  - `port` – порт балансировщика.

  > Другие форматы ввода URL-адреса балансировщика не допускаются.

5. Нажмите **Сохранить**.

Мониторинг сервисов

Вы можете использовать следующие возможности, чтобы отслеживать состояние всех сервисов, кроме холодного хранилища и агента:

- Просматривать алерты Victoria Metrics.

  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.
    - Красный – сервис не работает или не доступен с сервера Ядра.
    - Желтый – этот статус применяется ко всем сервисам, кроме агента. Желтый статус означает, что сервис работает, но в журнале сервиса есть ошибки или для сервиса есть алерты от Victoria Metrics. Сообщение об ошибке можно просмотреть, если навести курсор мыши на статус сервиса в разделе **Активные сервисы**.
    - 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 Victoria Metrics, статус сервиса будет желтым.
    - Серый – если в удаленном тенанте был работающий сервис, который продолжает работать, на странице Активные сервисы он будет отображаться с серым статусом. 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 Главному тенанту.

- Просматривать метрики Victoria Metrics 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 вы видите сообщение **Enrichment errors increasing**, вы можете выполнить следующие действия:

   - Перейти в раздел KUMA **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 вы видите сообщение **Output Event Loss increasing**, вы можете выполнить следующие действия:

   - Перейти в раздел KUMA **Метрики** → <тип сервиса> → <имя сервиса> → **IO** → **Output Event Loss** для сервиса в желтом статусе и просмотреть график, чтобы уточнить когда именно началась проблема и отследить 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 веб-консоли KUMA перейдите в раздел **Параметры** → **Другое** → **Мониторинг сервисов**.

2. 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.

3. 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 будет список сервисов с ошибками. Использование специальных символы ", },{, для поиска недопустимо, результаты будут нерелевантны.

Отключение мониторинга сервисов

Чтобы отключить мониторинг сервисов:

1. В веб-консоли KUMA перейдите в раздел **Параметры** → **Другое** → **Мониторинг сервисов**.

2. 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.

3. 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 мониторинга работы сервисов KUMA, потока событий и корреляций в KUMA выполняется сбор и хранение большого количества данных. Для сбора, хранения и анализа данных используется решение VictoriaMetrics, представляющее собой СУБД в формате временных рядов.

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

В консоли KUMA в разделе **Метрики** представлены панели мониторинга с информацией о метриках и визуализацией ключевых параметров работы различных сервисов KUMA. Визуализация собранных метрик осуществляется с помощью решения Grafana. При выборе раздела **Метрики** открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA.

На каком хосте установлено Ядро KUMA?

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

Сервис Ядра KUMA выполняет настройку параметров VictoriaMetrics и Grafana автоматически, участие пользователя не требуется. Графики в разделе **Метрики** появляются с задержкой около 1,5 минуты. Если в разделе **Метрики** вы видите core:<номер порта>, это означает, что метрики получены с хоста, на котором было установлено Ядро KUMA. В прочих конфигурациях отображается имя хоста, с которого KUMA получает метрики.

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

Метрики коллектора

IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса

Название метрики	Описание
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных в секунду. Начиная с версии KUMA 4.2 счетчик Processing EPS учитывает и части события auditd, и финальное (склеенное) событие. По этой причине возможно увеличение значений метрики **Processing EPS**.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения в секунду.
Output Latency (задержка вывода)	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors (ошибки вывода)	Количество ошибок, возникших в секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss (потеря событий)	Количество событий, потерянных в 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.

Название метрики	Описание
Output Disk Buffer Size (размер дискового буфера)	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 (байты, принятые в сеть)	Количество байт, принятых в сеть в секунду.
Connector errors (ошибки коннектора)	Количество ошибок в логах коннектора.

Normalization (нормализация) – метрики, относящиеся к нормализаторам

Название метрики	Описание
Raw & Normalized event size (размер сырых и нормализованных событий)	Размер необработанного и нормализованного событий. Отображается медиана.
Errors (ошибки)	Количество ошибок нормализации, возникших за секунду.

Filtration (фильтрация) – метрики, относящиеся к фильтрам

Название метрики	Описание
EPS (события, обрабатываемые за секунду)	Количество событий, отправленных в обработку за секунду. При наличии фильтра в конфигурации сервиса коллектора события, удовлетворяющие условиям фильтра, отбрасываются, а в обработку отправляются только события, не удовлетворяющие этим условиям.

Aggregation (агрегация) – метрики, относящиеся к правилам агрегации

Название метрики	Описание
EPS (события, обрабатываемые в секунду)	Количество событий, полученных и созданных правилом агрегации за секунду. Эта метрика помогает определить эффективность правил агрегации.
Buckets (контейнеры)	Количество контейнеров в правиле агрегации.

Enrichment (обогащение) – метрики, относящиеся к правилам обогащения

Название метрики	Описание
Cache RPS (запросы к кешу в секунду)	Количество запросов, отправленных локальному кешу за секунду.
Source RPS (запросы к источнику в секунду)	Количество запросов, отправленных источнику обогащения за секунду. Данные собираются только для типов источника обогащения **dns** и **cybertrace**.
Source Latency (задержка источника)	Время в миллисекундах, затраченное на отправку запроса источнику обогащения и получение от него ответа. Отображается медиана.
Queue (очередь)	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors (ошибки)	Количество ошибок, возникших за секунду при отправке запросов источнику обогащения.

Process (процессы) – метрики, относящиеся к процессам

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.

Название метрики	Описание
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.

Метрики коррелятора

IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса

Название метрики	Описание
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных в секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения в секунду.
Output Latency (задержка вывода)	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors (ошибки вывода)	Количество ошибок, возникших в секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss (потеря событий)	Количество событий, потерянных в 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)	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 (скорость передачи данных в сеть в секунду)	Количество байт, переданных в сеть за 1 секунду.

Correlation (корреляция) – метрики, относящиеся к правилам корреляции

Название метрики	Описание
EPS (события, обрабатываемые в секунду)	Количество корреляционных событий, созданных правилом корреляции за секунду.
Buckets (контейнеры)	Количество контейнеров в правиле корреляции стандартного типа.
Rate Limiter Hits (лимит срабатываний)	Количество превышений правилом корреляции лимита срабатываний за секунду.
Active Lists OPS (запросы к активному листу в секунду)	Количество запросов на выполнение операций, отправленных активному листу за секунду, и сами операции.
Active Lists Records (записи в активном листе)	Количество записей в активном листе.
Active Lists On-Disk Size (размер на диске)	Размер активного листа на диске в байтах.
Context Tables OPS (количество операций с контекстными таблицами в секунду)	Количество обращений к контекстной таблице за 1 секунду с указанием операции.

Название метрики	Описание
Context Tables Records (записи в контекстной таблице)	Текущее количество записей в контекстной таблице.
Context Tables On-Disk Size (размер контекстной таблицы на диске)	Текущий размер контекстной таблицы на диске.

Enrichment (обогащение) – метрики, относящиеся к правилам обогащения

Название метрики	Описание
Cache RPS (запросы к кешу в секунду)	Количество запросов, отправленных локальному кешу за секунду.
Source RPS (запросы к источнику в секунду)	Количество запросов, отправленных источнику обогащения, например словарю, за секунду.
Source Latency (задержка источника)	Время в миллисекундах, затраченное на отправку запроса источнику обогащения и получение от него ответа. Отображается медиана.
Queue (очередь)	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors (ошибки)	Количество ошибок, возникших за секунду при отправке запросов источнику обогащения.

Response (ответ) – метрики, относящиеся к правилам реагирования

Название метрики	Описание
RPS (запросы в секунду)	Количество активаций правила реагирования за секунду.

Process (процессы) – метрики, относящиеся к процессам

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.

Метрики хранилища

IO (ввод-вывод) – метрики, относящиеся к состоянию узлов кластера ClickHouse

Название метрики	Описание
Output EPS (вывод событий)	Количество событий в секунду, которые были вставлены в узел ClickHouse или в дисковый буфер узла.
Output Latency (задержка вывода)	Задержка вставки пакета либо в узел ClickHouse, либо в дисковый буфер узла.
Output Errors (ошибки вывода)	Количество ошибок в секунду при вставке пакета в узел ClickHouse или в дисковый буфер узла.
Output Disk Buffer Size (размер дискового буфера)	Размер дискового буфера узла ClickHouse.
Output Event Loss (потеря событий)	Количество событий, которые были безвозвратно потеряны на каждом узле ClickHouse.
Batch size (размер пакета)	Размер пакета событий для вставки в узел ClickHouse.
Insert interval 5min Q1 (интервал вставки)	Длительность первого квартиля интервала вставки событий за последние 5 минут.

ClickHouse / General (общие параметры) – метрики, относящиеся к общим параметрам кластера ClickHouse

Название метрики	Описание
Active Queries (активные запросы)	Количество выполняемых запросов, отправленных кластеру ClickHouse. Эта метрика отображается для каждого экземпляра ClickHouse.
QPS (запросы в секунду)	Количество запросов, отправленных кластеру ClickHouse в секунду.
Failed QPS (безуспешные запросы в секунду)	Количество безуспешных запросов, отправленных кластеру ClickHouse в секунду.
Allocated memory (назначенная память)	Количество RAM, назначенное процессу ClickHouse (зависит от технических характеристик сервера и может выражаться, например, в ГБ или МБ).
Active parts (активные части)	Количество активных частей. Активные части – это данные (файлы на диске), которые используются для обработки запросов в настоящее время.
Detached parts (count) (количество отключенных частей)	Количество отключенных (отсоединенных) частей. Отключенные части – это данные, которые существуют на диске, но не участвуют в файловых операциях чтения и записи.
Detached parts (size) (размер отключенных частей)	Объем дискового пространства, который занимают отключенные части. Вы можете указать максимальное значение размера отключенных частей от 1% до 90%. По умолчанию установлено значение 1%. Если размер отключенных частей превышает установленное максимальное значение, KUMA присваивает желтый статус запущенному сервису хранилища в разделе **Активные сервисы**.

ClickHouse / Insert (вставка) – метрики, относящиеся к вставке событий в экземпляр ClickHouse

Название метрики	Описание
Insert EPS (вставка событий)	Количество событий, вставленных в экземпляр ClickHouse за секунду.
Insert QPS (запросы на вставку в секунду)	Количество запросов на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse за секунду. Если на метрике **Insert QPS** растет очередь из запросов и показатель превышает 1, мы рекомендуем посмотреть также значение метрики **Batch size**, чтобы скорректировать параметры буферизации хранилища в настройках конфигурации сервиса 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. В норме показатель метрики **Insert QPS** не превышает 1.
Failed Insert QPS (безуспешные запросы на вставку в секунду)	Количество безуспешных запросов на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse за секунду.
Delayed Insert QPS (отложенные запросы на вставку в секунду)	Количество отложенных запросов на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse за секунду. Запросы были отложены узлом ClickHouse из-за превышения мягкого лимита активных слияний.
Rejected Insert QPS (отклоненные запросы на вставку в секунду)	Количество отклоненных запросов на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse за секунду. Запросы были отклонены узлом ClickHouse из-за превышения жесткого лимита активных слияний.
Active Merges (активные слияния)	Количество активных слияний.
Distribution Queue (очередь распределения)	Количество временных файлов с событиями, которые не удалось вставить в экземпляр ClickHouse из-за того, что он был недоступен. Эти события невозможно найти с помощью поиска.

ClickHouse / Select (выборка) – метрики, относящиеся к выборке событий в экземпляре ClickHouse

Название метрики	Описание
Select QPS (запросы на выборку в секунду)	Количество запросов на выборку событий в экземпляре ClickHouse, отправленных кластеру ClickHouse за секунду.
Failed Select QPS (безуспешные запросы на выборку в секунду)	Количество безуспешных запросов на выборку событий в экземпляре ClickHouse, отправленных кластеру ClickHouse за секунду.

ClickHouse / Replication (репликация) – метрики, относящиеся к репликам узлов ClickHouse

Название метрики	Описание
Active Zookeeper Connections (активные подключения к Zookeeper)	Количество активных подключений к узлам кластера Zookeeper. При нормальной работе это число должно быть равным количеству узлов кластера Zookeeper.
Read-only Replicas (реплики read-only)	Количество реплик узлов ClickHouse в режиме read-only. При нормальной работе таких реплик узлов ClickHouse быть не должно.
Active Replication Fetches (активные процессы скачивания)	Количество активных процессов скачивания данных с узла ClickHouse при репликации данных.
Active Replication Sends (активные процессы отправки)	Количество активных процессов отправки данных узлу ClickHouse при репликации данных.
Active Replication Consistency Checks (активные процессы проверки консистентности)	Количество активных проверок консистентности данных на репликах узлов ClickHouse при репликации данных.

ClickHouse / Networking (сеть) – метрики, относящиеся к сети кластера ClickHouse

Название метрики	Описание
Active HTTP Connections (активные HTTP-подключения)	Количество активных подключений к HTTP-серверу кластера ClickHouse.
Active TCP Connections (активные TCP-подключения)	Количество активных подключений к TCP-серверу кластера ClickHouse.
Active Interserver Connections (активные подключения между серверами)	Количество активных служебных подключений между узлами ClickHouse.

Agents (агенты)

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.
Disk used (events) (используемое пространство диска с событиями)	Часть раздела /opt в процентах, занятая событиями.
Disk used (except events) (используемое пространство диска без событий)	Часть раздела /opt в процентах, занятая данными, за исключением событий.

Метрики Ядра KUMA

Raft – метрики, относящиеся к чтению и обновлению состояния Ядра KUMA

Название метрики	Описание
Lookup RPS (запросы на чтение в секунду)	Количество запросов на выполнение процедур чтения, отправленных Ядру KUMA за секунду, и сами процедуры.
Lookup Latency (время обработки запроса на чтение)	Время в миллисекундах, затраченное на выполнение процедур чтения, и сами процедуры. Отображается время для 99-ого процентиля процедур чтения. Один процент процедур чтения может выполняться дольше.

Название метрики	Описание
Propose RPS (запросы на обновление состояния в секунду)	Количество запросов на выполнение процедур обновления состояния Raft (SQLite), отправленных Ядру KUMA за секунду, и сами процедуры.
Propose Latency (время обработки запроса на обновление состояния)	Время в миллисекундах, затраченное на выполнение процедур обновления состояния Raft (SQLite), и сами процедуры. Отображается время для 99-ого процентиля процедур обновления состояния. Один процент процедур обновления состояния может выполняться дольше.

Data mining – метрики, относящиеся к сбору и анализу данных

Название метрики	Описание
Executing Rules (количество запущенных планировщиков)	Количество запущенных планировщиков для выполнения запросов сбора и анализа данных.
Queued Rules (количество планировщиков в очереди)	Количество планировщиков для выполнения запросов сбора и анализа данных в очереди.
Execution Errors (количество ошибок запуска планировщика)	Количество ошибок при выполнении запуска планировщика сбора и анализа данных.
Execution Latency (время выполнения)	Время выполнения запросов планировщика.

Tasks – метрики, относящиеся к мониторингу выполнения задач на Ядре KUMA

Название метрики	Описание
Active tasks (выполняемые задачи)	Количество выполняемых задач за единицу времени.
Task Execution latency (время выполняемых задач)	Время выполняемых задач в секундах.
Errors (количество ошибок)	Количество ошибок при выполнении задач.

API – метрики, относящиеся к API-запросам

Название метрики	Описание
RPS (запросы в секунду)	Количество API-запросов, отправленных Ядру KUMA за секунду.
Latency (задержка)	Время в миллисекундах, затраченное на обработку одного API-запроса к Ядру KUMA. Отображается медиана.
Errors (ошибки)	Количество ошибок, возникших за секунду при отправке API-запросов Ядру KUMA.

Notification Feed (фид уведомлений) – метрики, относящиеся к активности пользователей

Название метрики	Описание
Subscriptions (подписки)	Количество клиентов, подключенных к Ядру KUMA через SSE для получения сообщений сервера в реальном времени. Обычно это число равно количеству клиентов, использующих веб-интерфейс KUMA.
Errors (ошибки)	Количество ошибок, возникших в секунду при отправке уведомлений пользователям.

Schedulers (планировщики) – метрики, относящиеся к задачам Ядра KUMA

Название метрики	Описание
Active (активные)	Количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
Latency (задержка)	Время в миллисекундах, затраченное на выполнение задачи. Отображается медиана.
Errors (ошибки)	Количество ошибок, возникших в секунду при выполнении задач.
Alerts Queue (очередь алертов)	Количество алертов в очереди на вставку в базу данных.

IO (ввод-вывод) – метрики, относящиеся к состоянию узлов Ядра KUMA

Название метрики	Описание
Output Disk Buffer Size (размер дискового буфера)	Размер каждого из дисковых файловых буферов на узле Ядра KUMA для задач отправки событий аудита, мониторинга, сбора и анализа данных в корреляторы.

Process (процессы) – метрики, относящиеся к процессам

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.

Метрики агента KUMA

IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса

Название метрики	Описание
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных в секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения в секунду.
Output Latency (задержка вывода)	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors (ошибки вывода)	Количество ошибок, возникших в секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss (потеря событий)	Количество событий, потерянных в 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)	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 (байты, принятые в сеть)	Количество байт, принятых в сеть в секунду.

Process (процессы) – метрики, относящиеся к процессам

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.

Метрики маршрутизатора событий

IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса

Название метрики	Описание
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных в секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения в секунду.
Output Latency (задержка вывода)	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors (ошибки вывода)	Количество ошибок, возникших в секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss (потеря событий)	Количество событий, потерянных в 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)	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 (байты, принятые в сеть)	Количество байт, принятых в сеть в секунду.

Process (процессы) – метрики, относящиеся к процессам

Название метрики	Описание
Memory (память)	Использование RAM (RSS) в мегабайтах.
Disk BPS (считанные/записанные байты диска)	Количество байтов, считанных/записанных на диск за секунду.

Название метрики	Описание
Network BPS (байты, принятые/переданные по сети)	Количество байтов, принятых/переданных по сети за секунду.
Network Packet Loss (потеря пакетов)	Количество сетевых пакетов, потерянных за секунду.
GC Latency (задержка сборщика мусора)	Время в миллисекундах, затраченное на проведение цикла сборщика мусора GO (Garbage Collector). Отображается медиана.
Goroutines (горутины)	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS (операционная система) – метрики, относящиеся к операционной системе

Название метрики	Описание
Load (нагрузка)	Средняя нагрузка.
CPU (ЦП)	Загрузка центрального процессора в процентах.
Memory (память)	Использование RAM (RSS) в процентах.
Disk (диск)	Использование дискового пространства в процентах.

Метрики сервиса Метрики

Stats (статистика)

Название метрики	Описание
Version	Версия KUMA.
Total Datapoints	Общее количество точек данных в базе данных.
Ingestion rate	Скорость вставки данных в базу данных (количество точек данных в секунду).
Read requests	Частота запросов на чтение данных в базе данных.
Available CPU	Количество доступных ядер процессора.
Uptime	Продолжительность работы сервиса.
Active series	Количество активных временных рядов.
Disk space usage	Объем занятого дискового пространства.
Available memory	Объем доступной памяти на сервере.
Bytes per point	Средний размер точки данных (в байтах).

Overview (обзор)

Название метрики	Описание
Datapoints ingestion rate	Скорость вставки данных в базу данных (количество точек данных в секунду).
Requests rate	Частота HTTP-запросов по путям.
Active timeseries	Количество активных временных рядов.
Query duration 0.99 quantile	Время выполнения запросов (99-й процентиль).
Requests error rate	Частота ошибок HTTP-запросов.

Resource usage (использование ресурсов)

Название метрики	Описание
RSS memory % usage	Использование RSS памяти (в процентах).
RSS anonymous memory % usage	Использование анонимной RSS памяти (в процентах).
Memory usage	Использование памяти (куча, резидентная, системная).
CPU % usage	Загрузка процессора (в процентах).
Open FDs	Использование файловых дескрипторов.
CPU	Использование ядер процессора.
Goroutines	Количество горутин Go.
Disk writes/reads	Скорость чтения и записи на диск (байт/сек).
Threads	Количество потоков.
Disk write/read calls	Количество системных вызовов ввода/вывода.
TCP connections rate	Скорость создания TCP-соединений.
TCP connections	Активные TCP-соединения.
Network usage	Сетевой трафик (входящий/исходящий).
CPU spent on GC	Время, потраченное процессором на сборку мусора.
Go scheduling latency	Задержка планировщика Go.
Slow inserts %	Количество медленных вставок (в процентах).

Troubleshooting (устранение неполадок)

Название метрики	Описание
Churn rate	Частота появления новых временных рядов и исчезновения старых временных рядов.
Assisted merges	Вынужденные слияния, которые выполняются синхронно в потоке записи данных, когда фоновые процессы слияния не успевают обрабатывать накопившиеся части LSM-дерева.
Slow queries rate	Частота медленных запросов.
Cache miss ratio	Количество промахов кеша при поиске точек данных (в процентах).
Cache usage % by type	Использование кеша по типам.
Deduplication rate	Скорость дедупликации данных.
Samples dropped for last 1h	Удаленные точки данных за последний час.
Restarts	Количество перезапусков сервиса.

Storage (хранилище)

Название метрики	Описание
Datapoints ingestion rate	Скорость вставки точек данных (количество точек данных в секунду).
Disk space usage - datapoints	Объем дискового пространства, занятого точками данными.
Storage full ETA	Прогноз времени заполнения хранилища.
Pending data points	Количество точек данных, ожидающих записи.
Datapoints	Количество точек данных по типам хранения.
LSM parts max by type	Максимальное количество частей LSM-дерева по типам.
Rows ignored for last 1h	Количество отброшенных строк за последний час.
Active merges	Количество активных слияний данных.

Название метрики	Описание
Concurrent flushes on disk	Параллельные записи данных на диск.
Merge speed	Скорость слияния данных.
Series read per query	Среднее количество рядов на один запрос.
Datapoints read per series	Среднее количество точек данных на один ряд.
Datapoints read per query	Среднее количество точек данных в расчете на один запрос.
Datapoints scanned per query	Количество просканированных точек данных в расчете на один запрос.

Alerting (алертинг)

Название метрики	Описание
Config error	Статус ошибки конфигурации.
Errors	Частота ошибок по правилам алертинга.
Alerting rules	Количество правил алертинга.
Alerts fired total	Всего сработавших алертов.
Top 10 groups by evaluation duration	Топ-10 групп правил алертинга по времени выполнения.
Rules execution rate	Частота выполнения правил алертинга.
Rules execution errors	Ошибки во время выполнения правил алертинга.
Missed evaluations	Пропущенные проверки правил алертинга.
Top 10 active alerts	Топ-10 активных алертов по правилам алертинга.

Метрики, относящиеся к тенантам

Tenants Overview – метрики, относящиеся к тенантам

Название метрики	Описание
License EPS (событий в секунду по условиям лицензии)	Количество событий в секунду, поступающих в рамках тенанта.

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.

https://rutube.ru/video/7f83843db68a555bd4ad72b4ee687c07/

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 собирает информацию от сервисов KUMA каждые 15 секунд.
- VictoriaMetrics обновляет алерты для сервисов KUMA каждую минуту.
- Сервис Ядро KUMA собирает информацию от VictoriaMetrics каждые 15 секунд.

Таким образом общая длительность задержки в обновлении статуса сервиса может достигать не более 2-3 минут.

Если вы отключили 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 пришел по API запросу в параметре /status от ClickHouse;
  - если холодное хранилище сервиса Хранилище не проверяется.

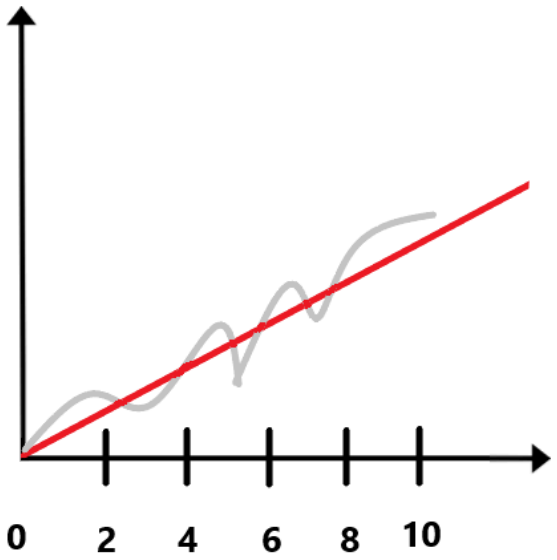
- Для сервиса коллектор: если алерт пришел по API-запросу в параметре /status.
- Для сервиса коррелятор: если есть правило реагирования, для которого требуется модуль Advanced Responses, но этот модуль отсутствует в действующей лицензии или срок действия лицензии, в которой есть этот модуль, истек.

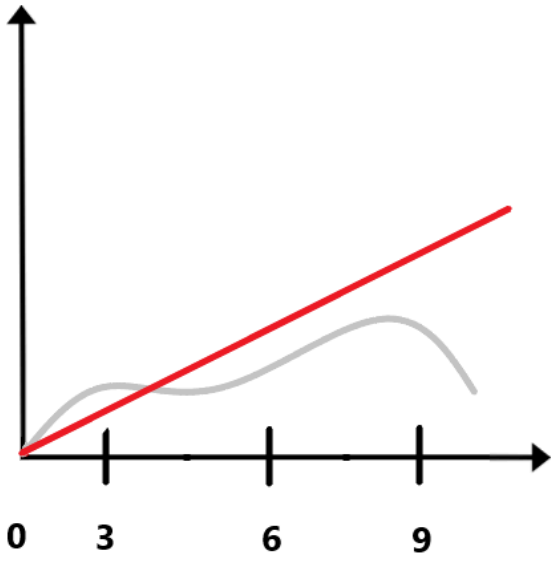
В таблице ниже представлена информация о том, какие сообщения об ошибке могут появиться в статусе сервиса при получении алерта от VictoriaMetrics и как и на основании каких метрик и параметров они рассчитываются. Подробнее о метриках KUMA, на основании которых могут сработать алерты VictoriaMetrics, 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").

Описание сообщений об ошибках для сервисов 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, на котором установлена 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.

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика KUMA	Описание
`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**.
`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). 

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика KUMA	Описание
`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. 
`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**.

Работа с задачами KUMA

При работе в веб-интерфейсе решения вы можете выполнять различные операции с помощью задач. Например, вы можете выполнить импорт активов или экспортировать информацию о событиях KUMA в TSV-файл.

Вы можете запускать несколько задач одновременно. Если вы запустили задачи разных типов, они выполняются параллельно в рамках одного тенанта. Задачи одного типа можно запускать одновременно только в разных тенантах. При попытке запустить несколько задач одного типа в одном тенанте выполняется только первая запущенная задача.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Диспетчер задач** окна веб-интерфейса решения.

Возможность просматривать задачи других пользователей зависит от роли пользователя. Пользователь с ролью Главного администратора может просматривать задачи всех пользователей. У пользователей с ролями на чтение и редактирование общих ресурсов нет доступа к задачам. Пользователям с другими ролями, включая пользователей с ролью Администратора тенанта, доступны для просмотра все задачи в доступных тенантах.

По умолчанию в разделе **Диспетчер задач** установлен флажок **Отображать только свои**. Для просмотра всех задач нужно снять флажок.

В таблице задач содержится следующая информация:

- **Статус** – статус задачи. Задаче может быть присвоен один из следующих статусов:
  - **Выполняется** – задача активна.

    Вы можете остановить выполнение задачи типа **Выполнение запроса в фоне** в статусе **Выполняется** по кнопке **Остановить и перезапустить в событиях**. После нажатия кнопки и подтверждения действия открывается раздел **События**, где запрос будет выполняться в обычном режиме.
  - **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 решении доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий KUMA.
  - **Выполнение запроса в фоне** – задача на выполнение SQL-запроса в фоновом режиме.
  - **Ретроспективное сканирование** – задача для проверки исторических событий.
  - **Threat Lookup** – запрос данных от портала Kaspersky Threat Intelligence Portal.
  - **Импорт активов KSC** – импорт информации об активах с серверов Kaspersky Security Center.
  - **Импорт атрибутов активов KSC** – импорт информации об атрибутах активов Kaspersky Security Center.
  - **Импорт активов KICS/KATA** – импорт информации об активах из KICS/KATA.
  - **Импорт учетных записей** – импорт информации о пользователях из Active Directory.
  - **Запуск программы через KEDR** – запуск произвольной программы с помощью Kaspersky Endpoint Detection and Reponse.

- **Обновление репозитория** – обновления репозитория KUMA для получения пакетов с ресурсами из указанного в параметрах источника.
- **Обновление политик мониторинга** – обновление параметров политики мониторинга.
- **Очистка истории изменений ресурсов** – удаление данных об изменениях в ресурсах.
- **Экспорт источников событий** – экспорт источников событий в формате CSV.
- **Запрос в KIRA** – запрос на анализ команды с помощью Kaspersky Investigation & Response Assistant.
- **Резервное копирование партиций** – задача резервного копирования партиций по расписанию и вручную.
- **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**.
- **Создано** – дата и время создания задачи.
- **Последнее обновление** – дата и время обновления задачи.
- **Тенант** – название тенанта, в котором была запущена задача.

Формат даты зависит от языка локализации, выбранного в параметрах решения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Настройка отображения таблицы задач

Вы можете настроить отображение столбцов, а также порядок их следования в таблице задач.

Чтобы настроить отображение в таблице задач:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. В заголовочной части таблицы нажмите на значок шестеренки (⚙).

3. В открывшейся панели выполните следующие действия:

   - Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.
   - Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите сбросить параметры, нажмите на ссылку **По умолчанию**.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на название столбца, зажмите левую клавишу мыши и перетащите столбец в нужное место.

Отображение столбцов в таблице задач будет настроено.

Просмотр результата выполнения задачи

Чтобы просмотреть результат выполнения задачи:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Выполните одно из следующих действий:

   - Для задач типа **Экспорт событий** и **Экспорт источников событий** нажмите на ссылку с типом задачи в столбце **Задача** и выберите **Скачать**.

     Результаты выполнения задачи будут загружены в виде файла в формате TSV.

   - Для задач типа **Выполнение запроса в фоне** нажмите на ссылку с типом задачи в столбце **Задача**. В новой вкладке браузера откроется раздел **События** с результатом выполнения SQL-запроса.

   - Нажмите на имя пользователя, создавшего задачу, или **Задача по расписанию** в столбце **Создал**.

     В открывшейся боковой панели будут представлены результаты выполнения задачи.

> Результаты выполнения задач типа **Обновление репозитория** не отображаются.

KUMA представляет результаты выполнения задач в зависимости от типа задачи. Например, для **Threat Lookup** отображается информация о типе обнаруженного объекта, приводятся данные о файле, обнаружениях и путях доступа. Для задач **Импорт активов KSC** и **Импорт активов KICS/KATA** показываются данные о тенанте и количестве скачанных объектов. Для задачи **Запрос в KIRA** приводятся данные о статусе задачи, даты отправки запроса и получении ответа, а также ссылка на событие.

> В этом разделе по умолчанию установлен флажок **Отображать только свои** в столбце **Создал**. Для просмотра всех задач вам необходимо снять этот флажок.

Повторный запуск задачи

Чтобы перезапустить задачу:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Установите флажок рядом с задачей, которую нужно перезапустить.

3. Нажмите на кнопку **Перезапустить**.

   Задача будет запущена повторно.

Подключение к SMTP-серверу

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Пользователи будут получать уведомления, если в свойствах 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 разделе веб-интерфейса KUMA **Параметры** → **Другое** → **Общие** → **Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Другое** → **Общие**.

2. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:

   - **Состояние** – выключите этот переключатель, 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** – отличное от FQDN название сервера Ядра KUMA, которое используется в вашей сети.

   - 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 на протяжении всего времени, когда источник в красном статусе. При этом уведомление о срабатывании политики мониторинга будет отправлено каждый раз, когда статус источника будет сменяться с красного на зеленый.

- Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен. Если на момент включения уведомлений в KUMA есть источники событий с красным статусом и вы еще не получали об этом уведомлений, вы получите одно уведомление за весь период, даже если на время отключения уведомлений мониторинга статус источников менялся несколько раз.

3. Нажмите **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 программных модулей или запускать на них антивирусную проверку с помощью задач Kaspersky Security Center. Задачи запускаются в веб-интерфейсе 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. **Создание задач 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 программы Kaspersky Endpoint Security для Windows или Linux. Задачи создаются в Kaspersky Security Center Web Console.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Windows см. в справке *Kaspersky Endpoint Security для Windows*.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Linux см. в справке *Kaspersky Endpoint Security для Linux*.

Название 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 веб-интерфейсе 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 программы Kaspersky Endpoint Security для Windows или 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 разделе **Активы** веб-интерфейса KUMA выберите актив, импортированный из Kaspersky Security Center.

   Откроется окно **Информация об активе**.

2. Нажмите на кнопку **Реагирование KSC**.

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 программы Kaspersky Endpoint Security для Windows или 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 веб-интерфейсе 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 срабатывания** 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 события выберите DeviceProduct.
5. В поле оператор выберите =.
6. В поле **Правый операнд** выберите **константа**.
7. В поле **значение** введите KSC.

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 имя события, при обнаружении которого вы хотите автоматически запускать задачу.

   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 веб-интерфейсе 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 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 веб-интерфейсе 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 KSC**.

6. В раскрывающемся списке **Задача Kaspersky Security Center** выберите задачу Kaspersky Security Center, которую требуется запустить.

7. В раскрывающемся списке **Поле события** выберите DestinationAssetID.

8. В поле **Обработчики** укажите 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.

9. В поле **Описание** вы можете добавить до 4000 символов в кодировке Unicode.

10. 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 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 веб-интерфейсе 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 сервисы**.

9. Нажмите на кнопку **Сохранить**.

Правило реагирования будет добавлено в коррелятор.

Автоматический запуск задачи обновления антивирусных баз и модулей программы 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 веб-интерфейсе 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 Kaspersky Security Center, и нажмите на кнопку **Перейти к событиям**.

   Откроется новая вкладка браузера в разделе **События** KUMA. В таблице отобразятся события с сервера 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.

Уведомления KUMA

Уведомления в веб-интерфейсе KUMA

По умолчанию для всех пользователей установлен флажок **Уведомлять об алертах в веб-интерфейсе** и в веб-интерфейсе KUMA отображаются уведомления об алертах.

При необходимости отображение таких уведомлений можно выключить, сняв флажок в профиле пользователя.

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**. Только пользователь с ролью Главный администратор может получать уведомления по почте.

Если для пользователя с ролью Главный администратор установлен флажок **Получать уведомления по почте**, раз в 6 часов с момента включения настройки пользователю будет отправлено уведомление по электронной почте по следующему правилу:

- Если на момент отправки письма есть хотя бы один сервис у которого поле Warning не пусто, письмо с уведомлением будет отправлено.
- Одно письмо на все сервисы с желтым статусом. Если нет сервисов с желтым статусом, письмо не будет отправлено.

Интервал в 6 часов будет соблюдаться, если не будет перезапуска Ядра KUMA. После каждого перезапуска Ядра отсчет 6-часового интервала начинается заново.

KUMA автоматически уведомляет пользователей о следующих событиях:

- создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета);
- создан алерт (уведомление получают все пользователи);
- алерт назначен пользователю (уведомление получает пользователь, которому был назначен алерт);
- выполнена задача (уведомление получают пользователи, создавшие задачу);
- доступны новые пакеты с ресурсами, которые можно получить путем обновления репозитория KUMA (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи);
- превышено среднесуточное количество EPS, ограниченное лицензией;
- превышено среднечасовое количество EPS, ограниченное лицензией SMB.

Пользовательские уведомления

Вместо стандартных уведомлений KUMA о создании алертов можно рассылать уведомления на основании пользовательских шаблонов. Настройка пользовательских уведомлений взамен стандартных происходит по шагам:

- Создание шаблона электронной почты.
- Создание правила уведомления, в котором указываются правила корреляции и адреса электронной почты.

Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

[▷]

https://rutube.ru/video/3aadb7010e5aaffca1a529456a8a35e9/

Журналы KUMA

В KUMA предусмотрены следующие типы журналов:

- Журналы установщика.
- Журналы компонентов.

Вы также можете создать отчет с диагностическими данными о вашем устройстве с помощью утилиты collect.sh. Подробную информацию о работе с утилитой см. в Базе знаний.

Журналы установщика

KUMA автоматически создает файлы с журналами установки, изменения конфигурации или удаления.

Журналы хранятся в папке ./log/ в директории установщика. В названии файла журнала используется дата и время запуска соответствующего скрипта.

Названия формируются в следующих форматах:

- Журнал установки: install-YYYYMMDD-HHMMSS.log. Например, install-20231031-102409.log
- Журналы удаления: uninstall-YYYYMMDD-HHMMSS.log. Например, uninstall-20231031-134011.log
- Журналы изменения конфигурации: expand-YYYYMMDD-HHMMSS.log. Например, expand-20231031-105805.log

При каждом запуске скрипта установки, изменения конфигурации или удаления KUMA создает новый файл. Ротация или автоматическое удаление журналов не предусмотрено.

Журнал содержит строки файла инвентаря, использованного при вызове соответствующей команды, и журнал ansible. Для каждой задачи последовательно отображается время запуска задачи (Вторник 31 октября 2023 10:29:14 +0300), время выполнения предыдущей задачи (0:00:02.611) и общее время с момента запуска установки, изменения конфигурации или удаления (0:04:56.906).

Пример:

TASK [Add columns to the replicated table] **********

Вторник 31 октября 2023 10:29:14 +0300 (0:00:02.611) 0:04:56.906 *******

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**.

Журналы Ядра хранятся в директории /opt/kaspersky/kuma/core/<`идентификатор сервиса Ядра KUMA`>/log/core и архивируются при достижении размера 5 ГБ или срока жизни 7 дней, в зависимости от того, что наступит раньше. Проверка выполнения условий выполняется ежедневно. 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. При высоком темпе заполнения журналов необходимо иметь достаточно места на диске для создания копии файла журнала и ее архивирования при ротации.

Журналы компонентов пополняются, пока файл 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:

Ядро	Как включить: в веб-интерфейсе KUMA в разделе **Параметры** → **Другое** → **Общие** → **Параметры Ядра** → **Отладка**. Где хранятся: /opt/kaspersky/kuma/core/<`идентификатор сервиса Ядра KUMA`>/log/core Журналы Ядра можно скачать в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы**. Для этого вам нужно выбрать сервис Ядра, нажать на значок меню (⋮) и выбрать **Скачать** → **Скачать журнал**. Если KUMA установлена в отказоустойчивой конфигурации, см. ниже раздел *Просмотр журналов Ядра в Kubernetes*.

Сервисы:
 	
• Хранилище
• Корреляторы
• Коллекторы
• Агенты
	Как включить: в параметрах сервиса с помощью переключателя **Отладка**.
	
	Где хранятся: в директории установки сервиса. Например, /opt/kaspersky/kuma/<`тип сервиса collector/correlator/storage`>/<`идентификатор сервиса`>/log/<`тип сервиса collector/correlator/storage`>. Журналы сервисов можно скачать в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы**. Для этого вам нужно выбрать нужный сервис, нажать на значок меню (⋮) и выбрать **Скачать** → **Скачать журнал**.
	
	Журналы на машинах Linux можно просмотреть с помощью команды journalctl и tail. Например:
	
	• Хранилище. Чтобы вернуть последние журналы из хранилища, установленного на сервере, выполните следующую команду:
	`journalctl -f -u kuma-storage-<идентификатор хранилища>`
	
	• Корреляторы. Чтобы вернуть последние журналы из корреляторов, установленных на сервере, выполните следующую команду:
	`journalctl -f -u kuma-correlator-<идентификатор коррелятора>`
	
	• Коллекторы. Чтобы вернуть последние журналы определенного коллектора, установленного на сервере, выполните следующую команду:
	`journalctl -f -u kuma-collector-<идентификатор коллектора>`
	
	• Агенты. Чтобы вернуть последние журналы агента, установленного на сервере, выполните следующую команду:
	`tail -f /opt/kaspersky/agent/<идентификатор агента>/log/agent`
	Работа агентов на машинах Windows журналируется всегда, если им присвоены права logon as a service, однако при установленном флажке **Отладка** данные указываются более подробно. 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 сервиса, к которому привязан ресурс, с помощью переключателя **Отладка**. Где хранятся: журналы хранятся на машине, на которой установлен сервис, использующий требуемый ресурс. Детализированные данные для ресурсов можно посмотреть в журнале сервиса, к которому привязан ресурс.

Просмотр журналов Ядра в Kubernetes

Файлы журналов Ядра архивируются, по достижении 100 Мб записывается новый журнал. Одновременно хранится не более пяти файлов. При появлении нового журнала, если файлов становится больше пяти, самый старый файл удаляется.

На рабочих узлах можно просмотреть журналы контейнеров и подов, размещенных на этих узлах, в файловой системе узла.
Например:
/var/log/pods/kuma_core-deployment-<UID>/core/*.log
/var/log/pods/kuma_core-deployment-<UID>/mongodb/*.log

Чтобы просмотреть журналы всех контейнеров пода core:

```
k0s kubectl logs -l app=core --all-containers -n kuma
```

Чтобы просмотреть журнал определенного контейнера:

```
k0s kubectl logs -l app=core -c <имя_контейнера> -n kuma
```

Чтобы включить просмотр журналов в реальном времени, добавьте ключ -f:

```
k0s kubectl logs -f -l app=core --all-containers -n kuma
```

Чтобы просмотреть журналы "предыдущего" пода, который был замещен новым, например, при восстановлении после критической ошибки или после повторного развертывания, добавьте ключ --previous:

```
k0s kubectl logs -l app=core -c core -n kuma --previous
```

Для доступа к журналам с других хостов, не входящих в кластер, необходим файл k0s-kubeconfig.yml с реквизитами доступа, который создается при установке KUMA, и локально установленная утилита управления кластером kubectl.
Контроллер кластера или балансировщик трафика, указанные в параметре server файла k0s-kubeconfig.yml, должны быть доступны по сети.

Путь к файлу необходимо экспортировать в переменную:
`export KUBECONFIG=/< путь к файлу >/k0s-kubeconfig.yml`

Для просмотра журналов можно использовать kubeclt, например:

```
kubectl logs -l app=core -c mongodb -n kuma
```

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`.

Описание CSV-файла

Имя заголовка поля в CSV	Описание поля	Пример
`Network`	IP-адрес в одном из следующих форматов: • единичный 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, его 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. Перед использованием архивы с файлами геоданных в CSV формате требуется конвертировать в поддерживаемый KUMA формат. Наименование конвертируемых CSV-файлов внутри архивов должно соответствовать шаблонам:

- (GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Blocks-IPv(4|6).csv
- (GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Locations-%s.csv

Конвертацию можно произвести с помощью приведенного ниже скрипта. Убедитесь, что CSV-файлы с геоданными не содержат дублирующихся записей: например, если в файле мало столбцов, в разные записи могут попадать данные одной и той же сети с теми же геоданными – такой файл конвертировать не удастся. Чтобы успешно выполнить конвертацию, убедитесь, что дублирующиеся строки отсутствуют и все строки уникальны по какому-либо полю.

Скачать 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","+
```

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 файл формата 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 веб-интерфейсе KUMA откройте раздел **Параметры** → **Другое** → **Общие**.

3. В блоке параметров **Геоданные** 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 веб-интерфейсе KUMA откройте раздел **Параметры** → **Другое** → **Общие**.

2. В блоке параметров **Геоданные** нажмите на кнопку **Экспортировать**.

Геоданные будут скачаны в виде CSV-файла (в кодировке UTF-8) с названием geoip.csv в соответствии с параметрами 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 отображается 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**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события, описанные ниже.

Соответствия по умолчанию для поля события SourceAddress

Атрибут геоданных	Поле события
Страна	`SourceCountry`
Регион	`SourceRegion`
Город	`SourceCity`
Широта	`SourceLatitude`
Долгота	`SourceLongitude`

Соответствия по умолчанию для поля события DestinationAddress

Атрибут геоданных	Поле события
Страна	`DestinationCountry`
Регион	`DestinationRegion`
Город	`DestinationCity`
Широта	`DestinationLatitude`
Долгота	`DestinationLongitude`

Соответствия по умолчанию для поля события DeviceAddress

Атрибут геоданных	Поле события
Страна	`DeviceCountry`
Регион	`DeviceRegion`
Город	`DeviceCity`
Широта	`DeviceLatitude`
Долгота	`DeviceLongitude`

Руководство пользователя

В этой главе представлены сведения о работе с SIEM-системой KUMA.

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. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов, на основе которых в свою очередь создаются сервисы KUMA.

Ресурсы содержатся в разделе веб-интерфейса KUMA **Ресурсы** в блоке **Ресурсы**. Доступные типы ресурсов:

- **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.
- **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.
- **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.
- **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 отбора отдельных событий из потока событий для дальнейшей их передачи в обработку.
- **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.
- **Шаблоны уведомлений** – ресурсы этого типа используются при рассылке уведомлений о новых алертах.
- **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 сервисам 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.

При нажатии на тип ресурса открывается окно, в котором отображается таблица с имеющимися ресурсами этого типа. Таблица содержит **следующие столбцы**:

Вы можете настроить набор столбцов таблицы и их порядок, а также настроить отображение данных в некоторых столбцах:

- Включить или выключить отображение столбцов можно в меню, открываемом с помощью нажатия на значок шестеренки (⚙) в панели инструментов в верхней части таблицы.

- Изменить порядок столбцов можно, перетаскивая заголовки столбцов влево либо вправо.

- Настроить отображение данных в столбце можно, нажав на значок стрелки вниз (⌄) в заголовке этого столбца.

- **Название** – название 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.

- **Тип** – тип ресурса. Отображается для всех типов ресурсов, кроме типов **Правила агрегации**, **Правила обогащения**, **Правила сбора и анализа данных**, **Фильтры**, **Активные листы**, **Прокси-серверы**.

- **Путь до ресурса** – адрес в дереве ресурсов. Отображается в дереве папок, начиная от тенанта, в котором создан ресурс.

- **Теги** – теги, которыми отмечен ресурс. Ресурс может иметь больше одного тега.

  > Теги являются частью ресурса и импортируются в случае импорта ресурса.

- **Название пакета** – имя пакета, из которого ресурс был импортирован из репозитория.

- **Коррелятор** – **список корреляторов, к которым привязано корреляционное правило**. Отображается только для ресурсов типа **Правила корреляции**.

  Если правило не привязано ни к одному коррелятору, в столбце отображается пустое значение. Если в списке есть несколько значений, то эти значения отсортированы в алфавитном порядке. Вы можете фильтровать значения в столбце **Коррелятор**, нажав на заголовок столбца и выбрав, какие правила корреляции вы хотите отображать в таблице: **Без коррелятора** или **С коррелятором**.

  > Для правил Общего тенанта отображаются корреляторы тенантов, к которым у вас есть доступ и которые вы выбирали в списке тенантов.

Значения в столбце **Коррелятор** доступны только для просмотра. Если вы хотите выполнить действия над корреляторами, вам нужно нажать на правило в таблице и в открывшихся свойствах этого правила перейти на вкладку **Корреляторы**.

- **Техники MITRE** – техники матрицы MITRE, которые покрывает это правило корреляции. Отображается только для ресурсов типа **Правила корреляции**. При наведении курсора мыши на значение отображается название правила.

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.

В таблице ресурсов в нижней части отображается количество ресурсов из доступных вам тенантов в таблице:

- **Всего** – общее количество или с учетом примененного фильтра или поиска.

- **Выбрано** – количество выбранных ресурсов.

При применении фильтров выбранные ресурсы и значение **Выбрано** сбрасываются. Если количество ресурсов изменится из-за действий другого пользователя (например, удаление), отображаемое количество ресурсов изменится после того, как вы обновите страницу, выполните действие с ресурсом или примените фильтр.

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, их 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 веб-интерфейса KUMA нажмите **Дублировать**, а затем нажмите **Сохранить**.

3. В веб-интерфейсе появится новый ресурс с названием [OOTB]<название_ресурса> - копия.

4. 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.

В таблице ресурсов в нижней части отображается количество ресурсов из доступных вам тенантов в таблице:

- **Всего** – общее количество или с учетом примененного фильтра или поиска.
- **Выбрано** – количество выбранных ресурсов.

При применении фильтров выбранные ресурсы и значение **Выбрано** сбрасываются. Если количество ресурсов изменится из-за действий другого пользователя (например, удаление), отображаемое количество ресурсов изменится после того, как вы обновите страницу, выполните действие с ресурсом или примените фильтр.

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. В структуре папок выберите нужную папку.
2. Правой кнопкой мыши вызовите контекстное меню и выберите **Удалить**.

   Появится окно подтверждения.
3. Нажмите **OK**.

Папка будет удалена.

> Решение 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 разделе **Ресурсы** → **<тип ресурса>** выберите или создайте папку, в которую требуется добавить новый ресурс.

   Корневые папки соответствуют тенантам. Чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.
2. Нажмите на кнопку **Добавить <тип ресурса>**.

   Откроется окно для настройки параметров выбранного типа ресурсов. Доступные параметры зависят от типа ресурса.
3. Введите имя ресурса в поле **Название**. Оно должно быть уникальным в рамках выбранного тенанта.
4. Укажите обязательные параметры (они отмечены красной звездочкой).
5. При желании укажите дополнительные параметры (это необязательное действие).
6. Нажмите **Сохранить**.

Ресурс будет создан и доступен для использования в сервисах и других ресурсах.

Чтобы переместить ресурс в новую папку:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажки рядом с ресурсами, которые вы хотите переместить. Можно выбрать сразу несколько ресурсов.

   Рядом с выбранными ресурсами отобразится значок ⣿. В нижней части таблицы отобразится количество выбранных ресурсов.
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 разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажок рядом с ресурсом, которые вы хотите скопировать, и нажмите **Дублировать**.

   В нижней части таблицы отобразится количество выбранных ресурсов.

   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 **Сохранить**.

Копия ресурса будет создана.

Чтобы изменить ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Выберите ресурс.

   Отображается окно с параметрами выбранного ресурса. Доступные параметры зависят от типа ресурса.
3. Измените нужные параметры.

4. Выполните одно из следующих действий:

   - Нажмите **Сохранить**, чтобы сохранить изменения.

   - Нажмите **Сохранить с комментарием** и в открывшемся окне укажите комментарий к сделанным изменениям. Изменения будут сохранены, и комментарий будет добавлен к созданной версии ресурса.

   Ресурс будет обновлен, и для него будет создана новая версия. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он задействовал новую версию ресурса.

   Если текущий ресурс недоступен для редактирования (например, невозможно изменить корреляционное правило), можно перейти в карточку другого ресурса, нажав на кнопку **Посмотреть**. Эта кнопка становится доступной в пакетных ресурсах при нажатии на другой ресурс, связанный с вашим текущим ресурсом.

Если при сохранении изменений ресурса обнаруживается, что текущая версия ресурса была изменена другим пользователем, вам будет предложен выбор из следующих действий:

- Сохранить ваши изменения как новую версию ресурса поверх изменений другого пользователя.

- Сохранить ваши изменения как новый ресурс.

  В этом случае будет создан дубликат изначального ресурса с измененными параметрами. В название нового ресурса будет добавлено `- копия`, и в комментарии к его версии будут указаны название и версия ресурса, с которого был создан дубликат.

- Отменить ваши изменения.

  Отмененные изменения невозможно восстановить.

Чтобы удалить ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.

2. Установите флажок рядом с ресурсом, которые вы хотите удалить, и нажмите **Удалить**.

   В нижней части таблицы отобразится количество выбранных ресурсов. Откроется окно подтверждения.

3. Нажмите **OK**.

   Ресурс и все его сохраненные версии будут удалены.

Массовое удаление ресурсов

В веб-интерфейсе KUMA имеется возможность множественного выбора ресурсов и их удаления.

У вас должны быть права на удаление ресурсов.

Чтобы удалить ресурсы:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемые ресурсы в структуре папок.

2. Установите флажок рядом с ресурсами, которые вы хотите удалить.

   В нижней части таблицы отображается общее количество ресурсов и количество выбранных ресурсов.

3. Нажмите **Удалить**.

Появится окно, в котором решение сообщает, можно ли безопасно удалить ресурсы, в зависимости от наличия связей выбранных для удаления ресурсов с другими ресурсами.

Для всех ресурсов, которые не могут быть удалены, решение отображает связи в табличном виде в модальном окне.

4. Нажмите **Удалить**.

   Удалятся только ресурсы без связей.

Удаление папок с ресурсами

Вы можете выбрать операцию удаления для любой папки, на любом уровне, кроме тенанта.

Чтобы удалить папку с ресурсами:

1. В разделе **Ресурсы** выберите папку.

2. Нажмите на кнопку ⋮ и выберите опцию **Удалить**.

   Откроется окно с запросом подтверждения удаления. В окне отобразится поле для ввода сгенерированного значения. Также при наличии зависимых ресурсов в папке отобразится список зависимостей.

3. Введите сгенерированное значение.

4. Подтвердите удаление.

Вы можете удалить папку, если:

- Папка не содержит вложенных папок и ресурсов.
- Папка не содержит вложенных папок, но содержит несвязанные ресурсы.
- Ни на один из ресурсов папки ничто не ссылается (сервисы, ресурсы, интеграции).

Привязка ресурсов к сервисам

Вы можете привязать ресурсы (правила корреляции, правила обогащения, правила реагирования, правила агрегирования и точки назначения) к таким сервисам, как коллекторы, корреляторы и маршрутизаторы событий. Доступные сервисы зависят от типа выбранного ресурса.

Чтобы привязать ресурс к сервису:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **<название 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 сервиса>**.

   Вы также можете привязать ресурс к сервису при изменении параметров ресурса. Для этого нажмите на название ресурса, перейдите на вкладку **Сервисы** и нажмите **Привязать к сервису** → **Привязать к <название сервиса>**.

При изменении параметров правила корреляции доступна вкладка **Корреляторы**, где вы можете привязать правило к корреляторам.

3. В открывшемся окне **<название сервиса>** установите флажки рядом с необходимыми сервисами и нажмите **OK**.

Ресурс будет привязан к сервису.

Чтобы отвязать ресурс от сервиса:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **<название ресурса>**.
2. Нажмите на ресурс и перейдите на вкладку **Сервисы**.

Для правил корреляции отображается вкладка **Корреляторы**.

3. Установите флажок рядом с каждым сервисом, от которого вы хотите отвязать ресурс.
4. Нажмите **Удалить** и подтвердите удаление привязки к сервису.

Ресурс будет отвязан от сервиса.

Обновление ресурсов

"Лаборатория Касперского" регулярно выпускает пакеты с ресурсами, доступные для импорта из репозитория. Вы можете указать адрес электронной почты в параметрах задачи **Обновление репозитория** и после первого выполнения задачи KUMA будет отправлять на указанный адрес уведомления о доступных для обновления пакетах. Вы можете выполнить обновление репозитория, проанализировать содержимое каждого обновления и принять решение об импорте и внедрении новых ресурсов в эксплуатируемую инфраструктуру. KUMA поддерживает обновление с серверов "Лаборатории Касперского" и из пользовательского источника, в том числе без прямого доступа к интернету с использованием механизма "зеркала обновления". При использовании в инфраструктуре других продуктов "Лаборатории Касперского", можно подключить KUMA к уже существующим зеркалам обновления. Подсистема обновления расширяет возможности KUMA по реагированию на изменения ландшафта угроз и инфраструктуры, а возможность ее использования без прямого доступа к интернету обеспечивает гарантии конфиденциальности данных, обрабатываемых системой.

Чтобы обновить ресурсы, вам необходимо выполнить следующие шаги:

1. Обновить репозиторий, чтобы доставить в репозиторий пакеты с ресурсами. Обновление репозитория доступно в двух режимах:
   - Автоматическое обновление.
   - Обновление вручную.
2. Импортировать пакеты с ресурсами из обновленного репозитория в тенант.

Чтобы сервис начал использовать обновленные ресурсы, после выполнения импорта убедитесь, что ресурсы привязаны. В случае необходимости привяжите ресурсы к коллекторам, корреляторам или агентам и обновите параметры.

Чтобы настроить автоматическое обновление:

1. В разделе **Параметры – Обновление репозитория** настройте **Интервал обновления в часах**. Значение по умолчанию - 24 часа.

2. Укажите **Источник обновления**. Доступны следующие варианты:

   - Серверы обновления "Лаборатории Касперского".

     Вы можете посмотреть список серверов обновления в Базе знаний.

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на хосте с установленным ядром KUMA.

       В случае использования локальной папки у системного пользователя kuma должен быть доступ для чтения к этой папке и ее содержимому.

3. При необходимости в поле **Прокси-сервер** выберите из списка существующий прокси-сервер, который должен использоваться при запуске задачи **Обновление репозитория**.

   Вы также можете создать новый прокси-сервер, нажав на значок плюса (+).

4. Укажите **Адреса электронной почты 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.

5. Нажмите **Сохранить**. Задача обновления запустится автоматически в самое ближайшее время и дальше запуск задачи будет выполнен в соответствии с расписанием.

Чтобы запустить обновление репозитория вручную:

1. Если вы хотите отключить автоматическое обновление, в разделе **Параметры – Обновление репозитория** установите флажок **Отключить автоматическое обновление**. По умолчанию флажок снят. 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 варианты:

   - Серверы обновления "Лаборатории Касперского".

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на хосте с установленным ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому.

3. При необходимости в поле **Прокси-сервер** выберите из списка существующий прокси-сервер, который должен использоваться при запуске задачи **Обновление репозитория**.

   Вы также можете создать новый прокси-сервер, нажав на значок плюса (+).

4. Укажите **Адреса электронной почты 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.

5. Нажмите **Запустить обновление**. Таким образом, вы одновременно сохраните настройки и вручную запустите выполнение задачи **Обновление репозитория**.

https://rutube.ru/video/ff4e4e2890023379682874042952 3e1f/

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 версии 4.2:

   - Выберите **Список программ**, затем нажмите на кнопку **Выбрать**. В открывшемся окне в разделе **Контроль периметра** установите флажок рядом с KUMA 4.2, 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_4_2=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 варианты:

   - Укажите локальную папку на хосте, где установлена Kaspersky Update Utility. Разверните HTTP-сервер, который будет отдавать обновления, и опубликуйте на нем эту локальную папку. В KUMA в разделе **Параметры** - **Обновление репозитория** - **Пользовательский источник** укажите URL к локальной папке, опубликованной на HTTP-сервере.

   - Укажите локальную папку на хосте, где установлена Kaspersky Update Utility. Сделайте эту локальную папку доступной по сети. Примонтируйте доступную по сети локальную папку на хосте с KUMA. В KUMA в разделе **Параметры** - **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 разделе **Ресурсы** нажмите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы** с деревом всех доступных ресурсов.

2. В поле **Пароль** введите пароль, который необходимо использовать для защиты экспортируемых данных.

3. В раскрывающемся списке **Тенант** выберите тенант, ресурсы которого вы хотите экспортировать.

4. Установите флажки рядом с ресурсами, которые вы хотите экспортировать.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы. В нижней части таблицы отображается количество выбранных ресурсов.

5. Нажмите на кнопку **Экспортировать**.

Текущие версии ресурсов в защищенном паролем файле сохранятся на вашем компьютере в зависимости от параметров вашего браузера. Предыдущие версии ресурсов не будут сохранены в файле. Ресурсы секретов экспортируются пустыми.

Чтобы экспортировать предыдущую версию ресурса:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** выберите необходимый тип ресурсов.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы** перейдите на вкладку **Список**.

2. Установите флажок напротив ресурса, историю изменений которого вы хотите просмотреть, и нажмите на кнопку **Показать историю версий** в верхней части таблицы.

   Откроется окно с историей версий ресурса.

3. Нажмите на строку версии ресурса, которую вы хотите экспортировать, и нажмите на кнопку **Экспорт** в нижней части открывшегося окна.

   Вы можете экспортировать только предыдущую версию ресурса. Кнопка **Экспорт** не отображается при выборе текущей версии ресурса.

Версия ресурса сохранится в файле JSON на вашем компьютере в зависимости от параметров вашего браузера.

Импорт ресурсов

При работе с KUMA 4.2 рекомендуется использовать ресурсы из пакета [OOTB] KUMA 4.2 resources и ресурсы, опубликованные в репозитории после выхода этого пакета.

KUMA поддерживает импорт ресурсов из более ранней версии в более позднюю, например из KUMA 3.4 в KUMA 4.0.

Чтобы импортировать ресурсы:

1. В разделе **Ресурсы** нажмите **Импорт ресурсов**.

   Откроется окно **Импорт ресурсов**.

2. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать импортируемые ресурсы.

3. В раскрывающемся списке **Источник импорта** выберите один из следующих вариантов:

   - **Файл**

     При выборе этого варианта необходимо указать пароль и нажать на кнопку **Импортировать**.

   - **Репозиторий**

При выборе этого варианта отображается список доступных для импорта пакетов. Мы рекомендуем убедиться, что дата обновления репозитория 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 с пометкой **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 следует сделать дубликат ресурса с помощью кнопки **Дублировать** и с дубликатом выполнить желаемые действия. При импорте следующих версий пакета дубликат не будет обновлен, поскольку он уже представляет собой отдельный объект.

Импортированные ресурсы, расположенные в папке `Integration`, можно изменить. Подобные ресурсы имеют пометку **Этот ресурс входит в пакет**. К пакетному ресурсу, размещенному в папке `Integration`, допускается добавление Словаря с типом `Таблица`, добавление иных ресурсов не допускается. При импорте следующих версий пакета измененный ресурс не будет заменен на аналогичный ресурс из пакета, что позволит сохранить внесенные изменения.

4. 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 – недоступна опция **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 другие 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 в разделе **Параметры** → **Поля расширенной схемы событий** или импортировать нормализатор, использующий необходимые поля.

Если в KUMA будет импортирован нормализатор, использующий поле расширенной схемы событий и такое поле уже существует в KUMA, будет использовано созданное ранее поле.

Если в KUMA будет импортирован нормализатор, использующий поле расширенной схемы событий, не соответствующее требованиям KUMA, импорт будет выполнен, но поле расширенной схемы событий будет создано со статусом **Выключено** и вы не сможете использовать это поле в других нормализаторах и ресурсах. Поле расширенной схемы событий не соответствует требованиям, например, если его имя содержит специальные символы или пробел. Если вы захотите использовать такое поле, не соответствующее требованиям, вам нужно исправить проблемы (например, изменить имя) и включить поле.

О разрешении конфликтов

Когда ресурсы импортируются в KUMA из файла, решение 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*.

При этом в случае конфликта импортируемый ресурс будет добавлен в качестве новой версии существующего ресурса. К этой версии будет добавлен комментарий *ресурс импортирован*.

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.

Поиск ресурсов

Вы можете искать ресурсы по названию или тегам. Вы также можете искать ресурсы по всем их полям с помощью полнотекстового поиска. Для типа ресурсов **Правила корреляции** доступен полнотекстовый поиск по корреляторам, в которых правила используются. При поиске по фильтру будут найдены все ресурсы, которые его используют.

Поиск осуществляется только по последней версии ресурсов.

Чтобы найти нужные ресурсы:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** выберите необходимый тип ресурсов.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы** перейдите на вкладку **Список**.

2. При необходимости, чтобы переключить режим поиска, нажмите на значок таблицы в верхней части таблицы ресурсов.

   Доступны поиск по названию, тегам и полнотекстовый поиск по всем полям ресурса. По умолчанию активен поиск по названию, тегам и корреляторам (только для правил корреляции).

   Вы можете определить, какой режим поиска активен, по тексту, который отображается в поле поиска по умолчанию.

3. В поле **Поиск** начните вводить текст поиска.

   Поиск инициируется во время ввода символов в поле и не чувствителен к регистру. В таблице отображаются только те ресурсы, которые удовлетворяют условиям поиска, и в нижней части таблицы отображается количество таких ресурсов.

   Для полнотекстового поиска результаты отсортированы по количеству слов в поисковой строке, найденных в полях ресурса, от большего к меньшему. KUMA выполняет поиск по JSON ресурса, если в нем указан другой ресурс, выполняет поиск по указанному ресурсу тоже. Если ресурс ссылается на другие ресурсы, KUMA также переходит в эти ресурсы и ищет по их содержимому.

4. Если вы хотите сбросить результат поиска, очистите поле **Поиск** или нажмите на значок ×.

Управление тегами

Для работы с ресурсами в веб-интерфейсе KUMA предусмотрена возможность добавлять теги для ресурсов, что позволяет вам осуществлять поиск нужного компонента, а также управлять тегами, отвязывать или привязывать теги.

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** → **Теги** и представлен в виде таблицы со следующими 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. Перейдите в раздел **Ресурсы** и выберите нужный ресурс.
2. В панели над таблицей нажмите **Добавить**.
3. В поле **Теги** выбранного ресурса добавьте новый тег или выберите тег из списка.
4. Нажмите **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 сервисов.

В результате поиска отображается список ресурсов и сервисов.

Чтобы найти нужные ресурсы по тегам:

1. Перейдите в раздел **Ресурсы** и выберите нужный 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 сервиса.
- Фильтровать ресурсы или сервисы по типу ресурса или сервиса, тегу.
- Привязать и/или отвязать теги.

Отображение тегов при добавлении зависимых ресурсов

При добавлении зависимого ресурса в выпадающем списке отображаются теги этого ресурса в разделе **Параметры фильтра**.

Теги ресурса, которые не вмещаются в одну строку, скрываются. О скрытых имеющихся тегах говорит специальный признак.

Фильтрация выпадающего списка осуществляется по наименованию ресурса и его тегам.

Привязка и отвязка тегов

Чтобы привязать теги к ресурсу или отвязать теги от ресурса:

1. Перейдите в раздел **Ресурсы**.
2. Выберите вкладку **Список**.
3. В столбце **Название** установите флажки рядом с необходимыми ресурсами.
4. В панели над списком выберите вкладку **Теги**.
5. Нажмите на кнопку **Привязать** или **Отвязать**, выберите необходимые теги или создайте новый тег.

   Выбранные теги будут привязаны к ресурсам или отвязаны от него.

   Вы также можете привязать или отвязать теги в карточке ресурса.

Трассировка использования ресурсов

Для устойчивой работы KUMA важно понимать, как одни ресурсы влияют на работоспособность других ресурсов, какие связи есть между ресурсами и другими объектами KUMA. Эти взаимозависимости вы можете отобразить визуально на интерактивном графе в веб-интерфейсе KUMA.

Отображение связей ресурса на графе

Чтобы отобразить связи выбранного ресурса:

1. В веб-консоли KUMA в разделе **Ресурсы** выберите тип ресурса.

   Отобразится список ресурсов выбранного типа.
2. Выберите необходимый ресурс.
3. В панели инструментов или в меню (⋮) нажмите на кнопку **Показать зависимости**.
4. Нажмите на кнопку **Показать зависимости**.

   Откроется окно графа зависимостей для выбранного ресурса. Если у вас нет прав на просмотр ресурса, то на графе он будет помечен значком (недоступный ресурс). При необходимости окно графа можно закрыть, чтобы вернуться к списку ресурсов.

Граф зависимостей ресурсов

На графе отображаются все связи, которые формируются на основе универсального уникального идентификатора (UUID) ресурсов, используемых в конфигурации ресурса, выбранного для отображения, а также связи ресурсов, которые имеют UUID выбранного ресурса в своей конфигурации. Связи "вниз", то есть ресурсы, на которые ссылается (использует) выбранный ресурс, показываются до последнего уровня, а связи "вверх", то есть ресурсы, которые ссылаются на выбранный ресурс – только на один уровень.

На графе вы можете посмотреть зависимости следующих ресурсов:

- правила корреляции;
- правила агрегации;
- правила обогащения;
- правила реагирования;
- правила data mining;
- нормализаторы;
- коннекторы;
- точки назначения;
- фильтры;
- панели мониторинга;

  Особенность отображения связей: у панелей мониторинга нет связи "вверх", так как панели мониторинга не входят в состав других ресурсов.

- шаблоны отчетов;

  Особенность отображения связей: у шаблонов отчетов нет связи "вверх", так как шаблоны отчетов не входят в состав других ресурсов.

- шаблоны уведомлений;
- активные листы;
- словари;
- прокси-серверы;
- секреты;
- контекстные таблицы;

- коллекторы;

  Особенность отображения связей: если для отображения связей был выбран, первично, коллектор, то связи "вверх" показываться не будут.

- корреляторы;

- хранилища;

- агенты (автоагенты);

  Особенность отображения связей: если выбран агент для отображения связей, то коллектор будет показан с типом связи **linked**, только если коллектор запущен как сервис и в агенте коллектор корректно (fqdn+port) указан в точке назначения.

- маршрутизаторы событий;

  Особенность отображения связей: если для отображения связей был выбран, первично, маршрутизатор событий, то связи "вверх" показываться не будут.

- интеграции;

  Название интеграции соответствует названию вкладки в разделе **Интеграции**.

- 0 (132) группа ресурсов;

  Число перед скобками указывает на количество отображенных на графе ресурсов из группы, число в скобках указывает на общее количество ресурсов в группе.

- недоступный ресурс (при отсутствии прав на просмотр).

При нажатии на узел ресурса вы можете посмотреть следующие данные о ресурсе:

- **Имя**

  Содержит ссылку на ресурс, при нажатии на ссылку этот ресурс открывается в отдельной вкладке, окно графа не закрывается.

- **Тип**

- **Путь**

  Путь ресурса без ссылки.

- **Теги**

- **Тенант**

- **Название пакета**

Вы можете открыть контекстное меню ресурса и выполнить следующие действия:

- Показать связи ресурса.

  Отобразятся зависимости выбранного ресурса.

- Скрыть ресурс на графе.

  Скрывается выбранный ресурс. Ресурсы уровня ниже, на которые ссылается выбранный ресурс, помечаются "*", как имеющие скрытые связи. Ресурсы, которые ссылаются на скрываемый ресурс, помечаются значком ссылки ( ), как имеющие скрытые связи. При этом граф разрывается.

- Скрыть связи "вниз" у этого ресурса на графе.

  Выбранный ресурс остается. Скрываются только те ресурсы нижнего уровня, у которых нет больше связей первого верхнего уровня на графе. Ресурсы, на которые ссылались ресурсы первого (скрываемого) уровня, помечаются "*", как имеющие скрытые связи.

- Скрыть все ресурсы этого типа на графе.

  Скрываются все ресурсы выбранного типа. Эта операция применяется для каждого ресурса выбранного типа.

- Обновить связи ресурса.

  Вы можете обновить состояние ресурса, если ресурс был изменен другим пользователем во время работы с графом. Отображается изменение только видимых связей.

- Сгруппировать.

  Если на экране нет узла группы: узел группы появляется на экране, ресурсы с типом выбранного ресурса, а также ресурсы, ссылающиеся на один ресурс, скрываются. Ребра перерисовываются от группы. Кнопка **Сгруппировать** доступна, только когда есть более 10 однотипных ссылок на ресурс.

  Если на экране есть узел группы: ресурс скрывается и добавляется в группу, ребра перерисуются от группы.

На графе отображаются несколько типов связи:

- Сплошная линия без надписи.

  Показывает прямую связь по UUID, в том числе использование секретов и прокси в интеграциях.

- Линия с надписью **<имя_функции>**.

  Показывает использование активного листа в корреляционном правиле.

- Пунктирная линия надписью **linked**.

  Показывает связь по URL, например, точки назначения с коллектором, или точки назначения с хранилищем.

Ресурсы, созданные инлайн, показываются на графе пунктирной линией с типом **linked**.

Не рекомендуется строить большие графы зависимостей. Рекомендуемое число узлов – до 100.

При открытии графа выбранный для просмотра ресурс будет некоторое время подсвечен мигающим кругом, так чтобы отличаться от остальных ресурсов графически и фокус внимания был именно на нем.

На графе вы можете посмотреть карту графа, чтобы понимать, в какой части графа вы находитесь. Вы можете воспользоваться селектором и передвигать его для отображения нужной части графа.

По кнопке **Упорядочить** вы можете улучшить отображение ресурсов на графе.

При выборе опции **Отобразить связи** фокус на графе не меняется, а ресурсы отображаются так, чтобы не пришлось возвращаться в начальное место.

При выборе на графе узла группы появляется боковая панель, в которой вы можете скрыть или отобразить ресурсы, входящие в группу. Для этого установите флажок рядом с нужным ресурсом и нажмите на кнопку **Отобразить на графе** или **Скрыть на графе**.

Граф сохраняет свое состояние, если пользователь отобразил что-то на графе, затем перешел в редактирование ресурса и снова открыл вкладку с графом.

Ранее отображенные ресурсы на графе остаются на своих местах при добавлении новых ресурсов на граф.

При закрытии графа все изменения сбрасываются.

После того, как связи ресурсов отрисованы на графе, вы можете осуществлять поиск узла:

- по имени;
- по тегу;
- по пути;
- по пакету.

Узлы, в том числе и группы, попадающие под критерий отбора, выделяются визуально – желтым кругом.

На графе вы можете использовать фильтр по типам ресурсов:

- Скрывать или отображать ресурсы определенного типа.
- Скрывать ресурсы нескольких типов. Отображать все типы ресурсов.

При закрытом окне фильтра можно увидеть выбранные фильтры по индикатору – красной точке в панели инструментов.

Ваши действия при работе с графом сохраняются в память (последние 50 действий), изменения можно отменить с помощью комбинации клавиш **`CTRL/COMMAND + Z`**.

Отображаемый граф можно сохранять в файл в формате SVG. В файле сохранится видимая часть графа.

Версионирование ресурсов

KUMA хранит историю изменения ресурсов в виде версий. Версия ресурса создается автоматически, когда вы создаете новый ресурс или сохраняете изменения параметров в существующем ресурсе.

> История изменений недоступна для ресурса **Словари**. Для хранения истории изменения словарей вы можете экспортировать данные.

Версии ресурсов хранятся в течение срока, указанного в разделе **Параметры**. Когда срок хранения версии ресурса достигает указанного значения, версия удаляется автоматически.

Вы можете просматривать историю изменений ресурсов KUMA, сравнивать версии, а также восстановить предыдущую версию ресурса, например, если необходимо восстановить его работоспособность.

Чтобы просмотреть историю изменений ресурса:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** выберите необходимый тип ресурсов.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы** перейдите на вкладку **Список**.

2. Установите флажок напротив ресурса, историю изменений которого вы хотите просмотреть, и нажмите на кнопку **Показать историю версий** в верхней части таблицы.

Откроется окно с таблицей сохраненных версий для выбранного ресурса. Для новых ресурсов существует только одна текущая версия.

Для каждой версии в таблице отображается следующая информация:

- **Версия** – порядковый номер версии ресурса. При сохранении изменений в ресурсе и создании новой версии порядковый номер увеличивается на 1.

  Версия с наибольшим номером и недавней датой публикации отражает актуальное состояние ресурса. Версия 1 отражает состояние ресурса при его создании.

- **Опубликовано** – дата и время, когда версия ресурса была создана.

- **Автор** – логин пользователя, сохранившего изменения ресурса.

  Если изменения были сделаны системой или с помощью скрипта миграции, отображается **system**.

- **Комментарий** – текстовый комментарий, указанный автором при сохранении изменений, или системный комментарий, описывающий сделанные изменения.

- **Срок хранения** – количество дней и дата, после которых версия ресурса будет удалена.

  При необходимости вы можете настроить срок хранения для версий ресурсов.

- **Действия** – кнопка восстановления версии ресурса.

Вы можете отсортировать таблицу версий ресурса по столбцам **Версия**, **Опубликовано** и **Автор**, нажав на заголовок и выбрав **По возрастанию** или **По убыванию**. Вы также можете отобразить в таблице изменения, сделанные только конкретным автором или авторами, нажав на заголовок столбца **Автор** и выбрав нужных авторов.

Если вы хотите просмотреть состояние ресурса в конкретной версии, вам нужно нажать на эту версию в таблице. Откроется окно с ресурсом этой версии, в котором вы можете выполнять следующие действия:

- просмотреть параметры, указанные в этой версии ресурса;

- восстановить эту версию ресурса, нажав на кнопку **Восстановить**;

- экспортировать эту версию ресурса в JSON-файл, нажав на кнопку **Экспорт**.

Сравнение версий ресурса

Вы можете сравнивать любые две версии ресурса, например, если вам нужно отслеживать внесенные изменения.

Чтобы сравнить версии ресурса:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** выберите необходимый тип ресурсов.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы** перейдите на вкладку **Список**.

2. Установите флажок напротив нужного ресурса и нажмите на кнопку **Показать историю версий** в верхней части таблицы.

   Откроется окно с историей версий ресурса.

3. Установите флажки напротив двух версий ресурса, которые вы хотите сравнить, и нажмите на кнопку **Сравнить** в верхней части таблицы.

Отобразится окно сравнения версий ресурса. Поля ресурсов отобразятся в виде списка или в формате JSON. Различия между двумя версиями будут выделены цветом. Вы можете выбрать другие версии для сравнения с помощью раскрывающихся списков над полями ресурсов.

Восстановление версии ресурса

Вы можете восстановить предыдущую версию ресурса, например, если вам нужно восстановить работоспособность ресурса в случае ошибок при внесении изменений.

Версии автоматически созданных агентов невозможно восстановить отдельно, так как они создаются при изменении родительского коллектора. Если вы хотите восстановить версию автоматически созданного агента, вам нужно восстановить соответствующую версию родительского коллектора.

Чтобы восстановить предыдущую версию ресурса:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** выберите необходимый тип ресурсов.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы** перейдите на вкладку **Список**.

2. Установите флажок напротив нужного ресурса и нажмите на кнопку **Показать историю версий** в верхней части таблицы.

   Откроется окно с историей версий ресурса.

3. В строке нужной версии в столбце **Действие** нажмите на кнопку **Восстановить**.

   Вы также можете восстановить версию, нажав на строку этой версии и нажав на кнопку **Восстановить** в нижней части окна.

   Вы можете восстановить только предыдущие версии ресурса; для текущей версии кнопка **Восстановить** недоступна.

Если после обновления KUMA изменилась структура ресурса, восстановление его сохраненных версий может быть недоступно.

4. Подтвердите действие и при необходимости укажите комментарий. Если вы не укажете комментарий, к версии автоматически будет добавлен комментарий *Восстановлена из версии v.<номер восстанавливаемой версии>*.

Версия ресурса будет восстановлена как новая версия и станет текущей.

Если ресурс, версию которого вы восстановили, добавлен в активный сервис, состояние сервиса также изменится. Необходимо перезагрузить сервис, чтобы применить изменение ресурса.

Настройка срока хранения версий ресурсов

Вы можете изменить срок хранения версий ресурсов в веб-интерфейсе KUMA в разделе **Параметры** → **Другое** → **Общие**, изменив значение параметра **Срок хранения истории ресурсов, дни**.

По умолчанию установлено значение 30 дней. Если вы хотите хранить все версии ресурсов без ограничений по сроку, вы можете использовать значение 0 (бессрочное хранение).

Только пользователь с ролью Главный администратор может просматривать и изменять срок хранения версий ресурсов.

Срок хранения версий ресурсов проверяется ежедневно, и версии ресурсов, которые хранятся в KUMA дольше указанного срока, удаляются автоматически. В разделе **Диспетчер задач** будет создана задача *Очистка истории изменений ресурсов* на проверку срока хранения версий ресурсов и удаление старых версий. Эта задача также запускается после перезапуска компонента Ядро.

Вы можете проверить время, оставшееся до удаления версии ресурса, в таблице версий в столбце **Срок хранения**.

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. Как правило, в роли точек назначения выступают коррелятор и хранилище.

Вы можете указать параметры точек назначения на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения.

Существуют следующие типы точек назначения:

- internal – используются для приема данных от сервисов KUMA по протоколу internal.
- nats-jetstream – используются для коммуникации через NATS.
- tcp – используются для связи по протоколу TCP.
- udp – используются для связи по протоколу UDP.
- http – используются для связи по протоколу HTTP.

- diode – используются для передачи событий с помощью диода данных.
- kafka – используются для коммуникаций с помощью kafka.
- file – используются для записи в файл.
- storage – используются для передачи данных в хранилище.
- correlator – используются для передачи данных в коррелятор.
- eventRouter – используются для передачи событий в маршрутизатор событий.

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, 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.

  Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом **internal**.
- События в маршрутизатор событий. Маршрутизатор событий может принимать события только по протоколу internal, поэтому при отправке событий в маршрутизатор событий вы можете использовать только точки назначения с типом **internal**.

Доступные параметры точки назначения с типом **internal** 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 – **internal**. Обязательный параметр.

Параметр	Описание
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: 16777216 (16 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 🖊.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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.

Параметр	Описание
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип nats-jetstream

Точки назначения с типом **nats-jetstream** используются для коммуникации через NATS. Доступные параметры точки назначения с типом **nats-jetstream** 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 – **nats-jetstream**. Обязательный параметр.

Параметр	Описание
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.
Тема	Тема сообщений NATS. Символы вводятся в кодировке Unicode. Обязательный параметр.
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша 🖊. **Как создать 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**.
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**.

Параметр	Описание

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.
	
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать 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**.
	
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

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 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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип tcp

Точки назначения с типом **tcp** используются для связи по протоколу TCP. Доступные параметры точки назначения с типом **tcp** 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 – **tcp**. Обязательный параметр.

Параметр	Описание
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.
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.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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**.

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 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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, 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-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.
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**.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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**.
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.

Параметр	Описание
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.
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип http

Точки назначения с типом **http** используются для связи по протоколу HTTP. Доступные параметры точки назначения с типом **http** 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 – **http**. Обязательный параметр.

Параметр	Описание
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.
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**.
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**.

Параметр	Описание

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.
	
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать 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**.
	
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

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
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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**.
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.
Путь	Путь, который требуется добавить в запрос к URL-адресу, указанному в поле **URL** на вкладке **Основные параметры**. Например, если вы укажете путь `/input`, а в качестве URL-адреса укажете `10.10.10.10`, от точки назначения будут исходить запросы `10.10.10.10/input`.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Путь проверки работоспособности	URL-адрес для отправки запросов для получения данных о работоспособности системы, с которой ресурс точки назначения устанавливает связь.
Проверка работоспособности	Переключатель, включающий проверку работоспособности. По умолчанию этот переключатель выключен.
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип diode

Точки назначения с типом **diode** используются для передачи событий с помощью диода данных. Доступные параметры точки назначения с типом **diode** 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 – **diode**. Обязательный параметр.

Параметр	Описание
Директория, из которой диод данных получает события	Путь к директории, из которой диод данных перемещает события. Максимальная длина пути составляет до 255 символов в кодировке Unicode. **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]:\\ProgramData\\Kaspersky Lab\\KUMA` Эти шаблоны используются системой для проверки пути. В них двойные обратные косые черты (\\) используются в качестве части синтаксиса регулярного выражения и не должны указываться в самом пути вручную. **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.

Параметр	Описание
	Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Пути, указанные в полях **Директория, из которой диод данных получает события** и **Временная директория**, не должны совпадать.
Временная директория	Путь к директории, в которой события готовятся для передачи диоду данных. Максимальная длина пути составляет до 255 символов в кодировке Unicode. События собираются в файл по истечении времени ожидания или при переполнении буфера. По умолчанию время ожидания составляет 10 секунд. Подготовленный файл с событиями перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**. В качестве названия файла с событиями используется хеш-сумма (SHA-256) содержимого файла с событиями. Пути, указанные в полях **Директория, из которой диод данных получает события** и **Временная директория**, не должны совпадать.
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.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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.
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип kafka

Точки назначения с типом **kafka** используются для коммуникаций с помощью kafka. Доступные параметры точки назначения с типом **kafka** 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 – **kafka**. Обязательный параметр.

Параметр	Описание
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.
Топик	Тема сообщений Kafka. Максимальная длина темы составляет до 255 символов. Вы можете использовать следующие символы: a–z, A–Z, 0–9, ".", "_", "-". Обязательный параметр.
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. • **PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать PFX-сертификат из хранилища, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**.
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.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Параметр	Описание
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**. • **LZ4**. • **zstd**. Если вы не выберете значение, сжатие будет выключено (значение по умолчанию).
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 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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип file

Точки назначения с типом **file** используются для записи в файл. Доступные параметры точки назначения с типом **file** описаны в таблицах ниже.

> При удалении точки назначения с типом **file**, используемой в сервисе, вам нужно перезапустить сервис.

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 – **file**. Обязательный параметр.

Параметр	Описание
URL	Путь к файлу, в который требуется 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/` 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**.
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.
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип storage

Точки назначения с типом **storage** используются для передачи данных в хранилище. Доступные параметры точки назначения с типом **storage** 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 – **storage**. Обязательный параметр.

Параметр	Описание
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 🖊.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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.

Параметр	Описание
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип correlator

Точки назначения с типом **correlator** используются для передачи данных в коррелятор. Доступные параметры точки назначения с типом **correlator** 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 – **correlator**. Обязательный параметр.

Параметр	Описание
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 🖊.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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.

Параметр	Описание
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип eventRouter

Точки назначения с типом **eventRouter** используются для передачи событий в маршрутизатор событий. Доступные параметры точки назначения с типом **eventRouter** 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 – **eventRouter**. Обязательный параметр.

Параметр	Описание
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 🖊.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом KUMA в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
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.

Параметр	Описание
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, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Предустановленные точки назначения

В поставку KUMA 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.

  Мы рекомендуем 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-адресу.

  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 веб-интерфейсе KUMA:

   - В разделе **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 с помощью кнопки **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 на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные 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 курсора мыши на кружок или блок, обозначающей 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. На блоке указаны условия, при котором дополнительное правило парсинга будет задействовано, название дополнительного правила парсинга, а также поле события, при наличии которого данные передаются в нормализатор. Параметры дополнительного правила парсинга можно просмотреть или изменить, нажав его блок.

Если навести курсор мыши на дополнительный нормализатор, отобразится кнопка со значком плюса, с помощью которой можно создать новое дополнительное правило парсинга событий. С помощью кнопки со значком корзины нормализатор можно удалить.

Дополнительные нормализаторы применяются сверху вниз до первого подошедшего условия.

Условия обработки события дополнительными нормализаторами

Если событие подошло под условия обработки дополнительными нормализатором, возможны следующие варианты:

- Событие обработано дополнительным нормализатором, тогда:

  1. После обработки событие передается на обработку дочерним дополнительным нормализаторам при их наличии.

  2. Обработанное событие возвращается в основной нормализатор и передается дальше по цепочке.

- Событие не обработано, произошла ошибка и для параметра **Сохранять исходное событие** в коллекторе указано значение параметра **При возникновении ошибок**, тогда:

1. Событие возвращается в основной нормализатор.

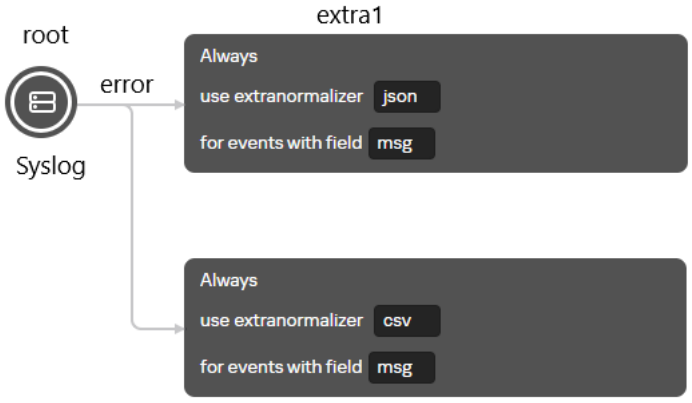
2. KUMA создает запись об ошибке в журнале коллектора.

3. Сырое событие записывается в поле **Raw**.

   Пример 1

   Предварительное условие

   Создан коллектор с нормализатором с параметром **Сохранять исходное событие** и значением параметра **При возникновении ошибок**.



Пример возникновения ошибки

   Результат

   Событие попадает в `extra 1 JSON`, только если соответствует условию отбора.

Дополнительный нормализатор `extra1 JSON` не сработал, возникла ошибка (см. рисунок выше). Обработка завершается, в журнале коллектора появляется запись об ошибке, сырое событие записывается в поле **Raw**.

Пример 2

Предварительное условие

Создан коллектор с нормализатором с параметром **Сохранять исходное событие** и значением параметра **При возникновении ошибок**.

Схема нормализации событий

Отправлено событие:

```
<1>May 31 11:55:21 srv-06 for_secondlvl_grp1[786]: Message=|test1|test2|;
```

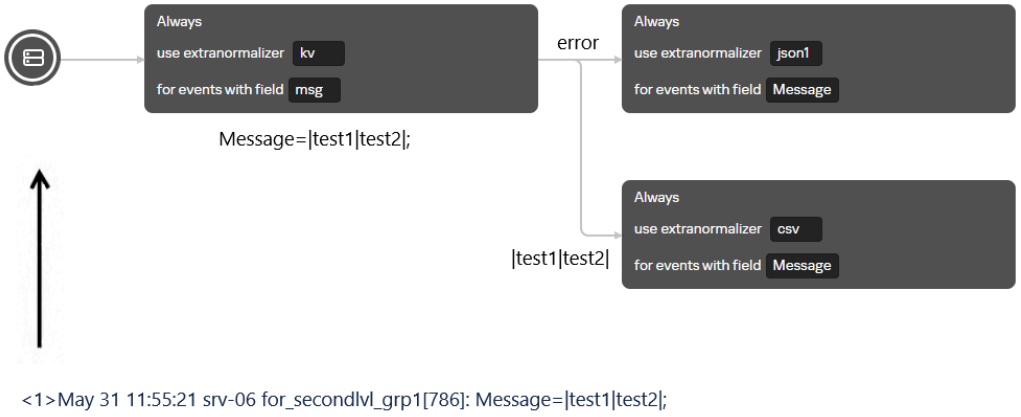


Схема возникновения ошибки

Результат

На втором уровне дополнительной нормализации `json1` возникла ошибка, обработка прерывается (см. рисунок выше).

В журнале коллектора появляется запись об ошибке, сырое событие записывается в поле **Raw**.

Пример 3

Предварительное условие

Создан коллектор с нормализатором с параметром **Сохранять исходное событие** и значением параметра **При возникновении ошибок**.

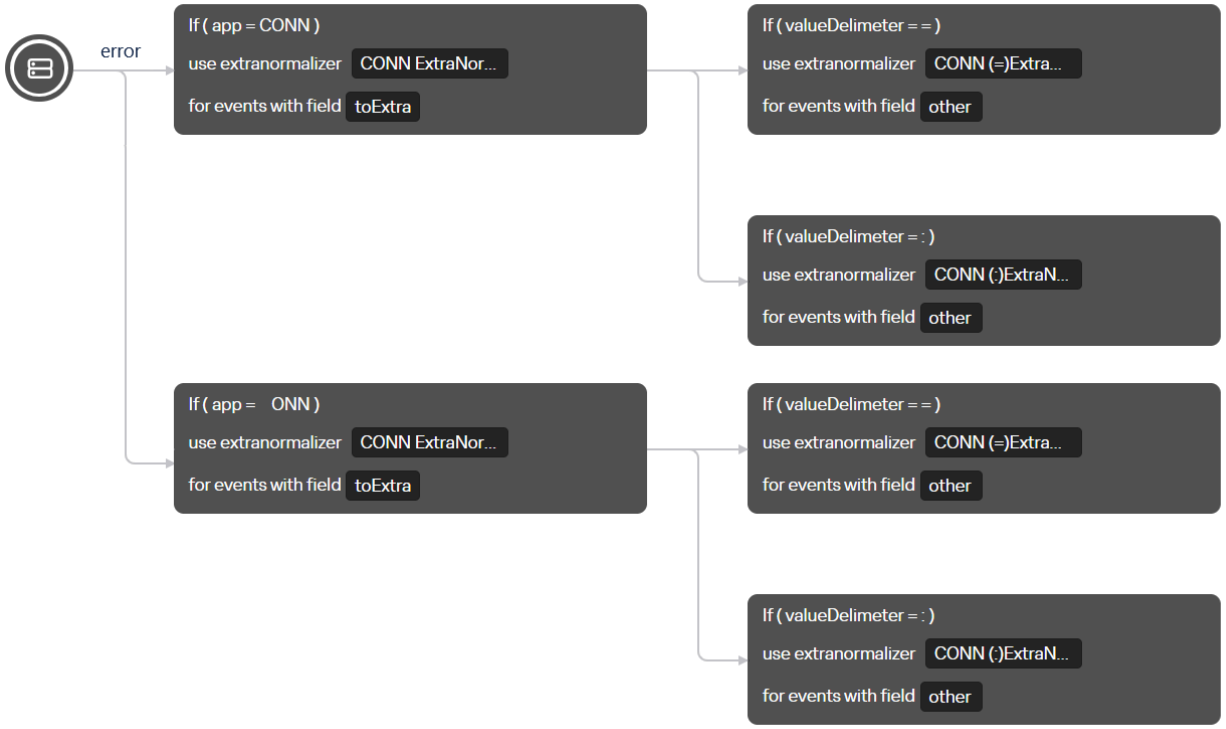


Схема возникновения ошибки

Результат

Дополнительный нормализатор уровня 1 не сработал, возникла ошибка (см. рисунок выше). Ветка этого дополнительного нормализатора прерывается и дочерние дополнительные нормализаторы уровня 2 не применяются.

Обработка события завершается, событие возвращается в основной нормализатор, в журнале коллектора появляется запись об ошибке, сырое событие записывается в поле **Raw**.

- Событие не обработано, поле переданное в дополнительный нормализатор пустое, для параметра **Сохранять исходное событие** в коллекторе указано значение параметра **При возникновении ошибок**, тогда:

  1. Событие возвращается в основной нормализатор.

  2. В журнале коллектора не регистрируется ошибка.

  3. Сырое событие не записывается в поле **Raw**.

     Пример 4

     Предварительное условие

Создан коллектор с нормализатором с параметром **Сохранять исходное событие** и значением параметра **При возникновении ошибок**.

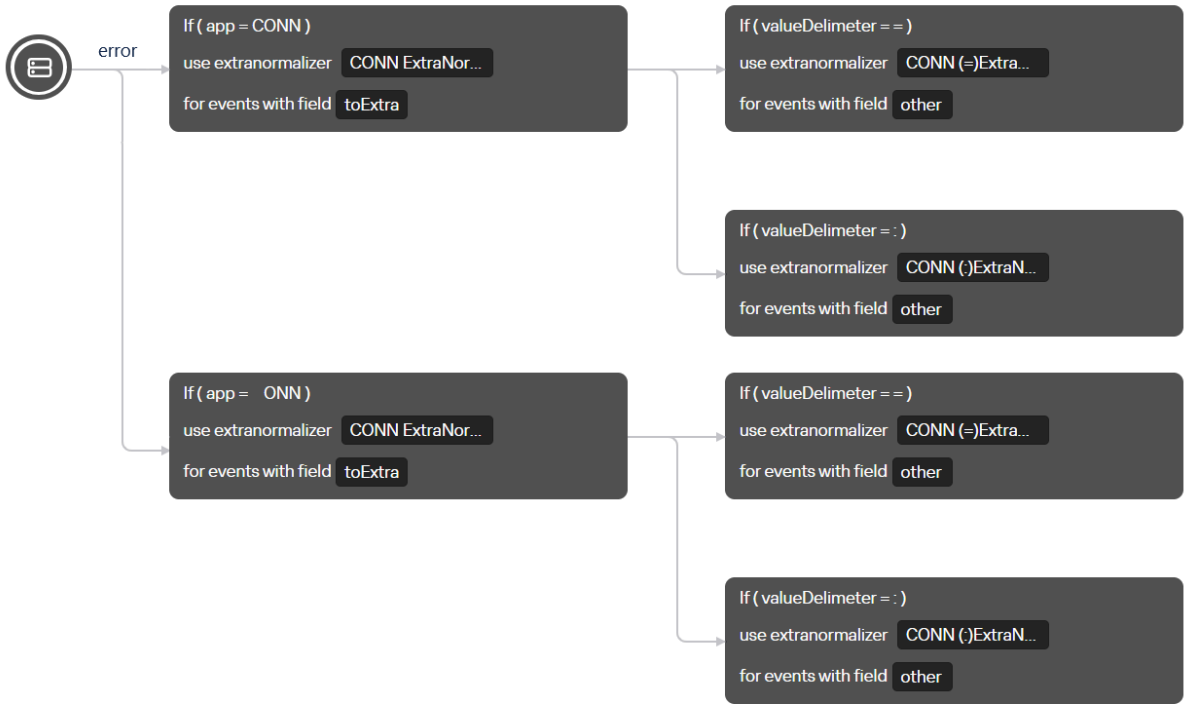


Схема возникновения ошибки

Результат

Поле, переданное в дополнительный нормализатор 1, пустое (см. рисунок выше).

Событие не обработано, событие возвращается в основной нормализатор, в журнале коллектора отсутствует запись об ошибке, сырое событие не записывается в поле **Raw**.

- Если событие не удовлетворяет условиям ни одного дополнительного нормализатора, для параметра **Сохранять исходное событие** в коллекторе указано значение параметра **При возникновении ошибок**, тогда:

  1. Сырое событие сохраняется в поле **Raw**.

  2. В журнале коллектора не регистрируется ошибка.

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. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы → Нормализаторы**.

https://rutube.ru/video/fcbf28d1d95e79d016535d9a37790010/

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. Доступные параметры парсинга событий описаны в таблице ниже.

При нормализации событий, помимо полей стандартной схемы событий KUMA вы также можете использовать поля расширенной схемы событий.

Доступные параметры парсинга событий

Параметр	Описание

Метод парсинга	Тип входящих событий. В зависимости от выбранного метода парсинга вы можете использовать преднастроенные правила сопоставления полей событий или задать свои правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, которые вам нужно заполнить. Доступные методы 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 вы можете обращаться к полям вложенных объектов, указывая названия параметров поочередно через точку. 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 неправильно. 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 обрабатываемое событие целиком передается в дополнительный нормализатор. В качестве разделителя строк вы можете использовать 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** в раскрывающемся списке **Использовать сырое событие** выберите **Да**. • **cef** Этот метод парсинга используется для обработки данных в формате CEF. При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. • **regexp** Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений. Вам нужно добавить регулярное выражение (синтаксис RE2) с именованными группами захвата в поле блока параметров **Нормализация**. Имя группы захвата и ее значение будут считаться полем и значением сырого события, которое можно будет преобразовать в поле события формата KUMA. *Чтобы добавить правила обработки событий:* 1. При необходимости в поле **Примеры событий** скопируйте пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг. 2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например `"(?P<name>regexp)"`. Регулярное выражение, добавленное в поле блока параметров **Нормализация**, должно полностью совпадать с событием. При разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: `^`, `$`. Вы можете добавить несколько регулярных выражений или удалить регулярные выражения. Для добавления регулярного выражения нажмите на кнопку **Добавить регулярное выражение**. Для удаления регулярного выражения нажмите рядом с ним на значок удаления ✕. 3. Нажмите на кнопку **Перенести названия полей в таблицу**. Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Вы можете выбрать соответствующее группе захвата поле KUMA в столбце напротив каждой группы захвата. Если вы именовали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF при нормализации**. Правила обработки событий будут добавлены. • **syslog** Этот метод парсинга используется для обработки данных в формате syslog. При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Для парсинга событий в формате rfc5424 с секцией `structured-data` вам нужно в раскрывающемся списке **Сохранить дополнительные поля** выбрать **Да**. В этом случае значения из секции `structured-data` станут доступны в полях `Extra`. • **csv** Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV. При выборе этого метода парсинга вам нужно в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя значений в строке можно использовать любой однобайтовый символ ASCII. • **kv** Этот метод парсинга используется для обработки данных в формате ключ-значение. Доступные параметры метода парсинга описаны в таблице ниже.

Доступные параметры метода парсинга

Параметр	Описание
Разделитель пар	Символ для разделения пар ключ-значение. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель значений**.
Разделитель значений	Символ для разделения ключа и значения. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель пар**.

- **xml**

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

При выборе этого метода парсинга вы можете указать ключевые атрибуты XML, которые требуется извлекать из тегов, в блоке параметров **Атрибуты XML**. Если в структуре XML в одном теге есть атрибуты XML с разными значениями, вы можете определить значение, указав ключ к значению в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML:

1. Нажмите на кнопку **+ Добавить поле**.

2. В открывшемся окне укажите путь к атрибуту XML.

Вы можете добавить несколько атрибутов XML и удалить атрибуты XML. Для удаления отдельного атрибута XML нажмите рядом с ним на значок удаления ✕. Для удаления всех атрибутов XML нажмите на кнопку **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Нумерация тегов

Начиная с версии KUMA 2.1.3 доступна автоматическая нумерация тегов в событиях в формате XML. Это позволяет распарсить событие с одинаковыми тегами или неименованными тегами, такими как `<Data>`.

В качестве примера мы используем нумерацию тегов атрибута `EventData` **события Microsoft Windows PowerShell event ID 800**.

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
   <System>
      <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-8497-
      1e730c959516}" EventSourceName="NTDS" />
      <EventID Qualifiers="0000">0000</EventID>
      <Version>@</Version>
      <Level>4</Level>
      <Task>15</Task>
      <Opcode>0</Opcode>
      <Keywords >0x8080000000000000</Keywords>
      <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
      <EventRecordID>55647</EventRecordID>
      <Correlation />
      <Execution ProcessID="1" ThreadID="1" />
      <Channel>service</Channel>
      <Computer>computer</Computer>
      <Security UserID="0000" />
   </System>
   <EventData>
      <Data>583</Data>
      <Data>36</Data>
      <Data>192.168.0.1:5084</Data>
      <Data>level</Data>
      <Data>name, lDAPDisplayName</Data>
      <Data />
      <Data>5545</Data>
      <Data>3</Data>
      <Data>0</Data>
      <Data>0</Data>
      <Data>0</Data>
      <Data>15</Data>
      <Data>none</Data>
   </EventData>
</Event>
```

Для парсинга событий с одинаковыми тегами или неименованными тегами вам нужно настроить нумерацию тегов и маппинг данных для пронумерованных тегов с полями события KUMA.

KUMA 3.0.x поддерживает одновременное использование атрибутов XML и нумерации тегов в рамках одного экстранормализатора. Если атрибут XML содержит неименованные теги или одинаковые теги, мы рекомендуем использовать нумерацию тегов. Если атрибут XML содержит только именованные теги, мы рекомендуем использовать атрибуты XML.

Для использования атрибутов XML и нумерации тегов в экстранормализаторах вам нужно последовательно включить параметр **Использовать сырое событие** в каждом экстранормализаторе по пути следования события в целевой экстранормализатор и в целевом экстранормализаторе.

В качестве примера работы нумерации тегов вы можете обратиться к нормализатору **MicrosoftProducts**. Параметр **Использовать сырое событие** включен последовательно в экстранормализаторах **AD FS** и **424**.

Чтобы настроить парсинг событий с неименованными или одинаковыми тегами:

1. Откройте существующий или создайте новый нормализатор.
2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите **xml**.
3. В поле **Нумерация тегов** нажмите на кнопку **+ Добавить поле**.
4. В отобразившемся поле укажите полный путь к тегу, элементам которого требуется присвоить порядковый номер, например `Event.EventData.Data`. Первому тегу будет присвоен номер 0. Если тег пустой, например `<Data />`, ему также будет присвоен порядковый номер.
5. Для настройки маппинга данных в группе параметров **Сопоставление** нажмите на кнопку **+ Добавить строку** и выполните следующие действия:
   a. В отобразившейся строке в поле **Исходные данные** укажите полный путь к тегу и индекс тега. Например, для события Microsoft Windows PowerShell event ID 800 из примера выше полные пути к тегам и индексы тегов будут выглядеть следующим образом:
      - `Event.EventData.Data.0`;
      - `Event.EventData.Data.1`;
      - `Event.EventData.Data.2` и так далее.
   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии KUMA, в которое попадет значение из пронумерованного тега после выполнения парсинга.
6. Сохраните изменения одним из следующих способов:
   - Если вы создали новый нормализатор, нажмите на кнопку **Сохранить**.
   - Если вы изменили существующий нормализатор, в коллекторе, к которому привязан нормализатор, нажмите на кнопку **Обновить параметры**.

Настройка парсинга будет завершена.

- **netflow**

  Этот метод парсинга используется для обработки данных во всех поддерживаемых форматах на основе протокола NetFlow: NetFlow v5, NetFlow v9 и IPFIX.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. При этом будут учтены исходные поля всех версий NetFlow (NetFlow v5, NetFlow v9 и IPFIX).

  Если метод парсинга **netflow** выбран для основного парсинга, дополнительная нормализация недоступна.

  > В правилах сопоставления по умолчанию для метода парсинга **netflow** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow5**

  Этот метод парсинга используется для обработки данных в формате NetFlow v5.

  При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

  > В правилах сопоставления по умолчанию для метода парсинга **netflow5** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow9**

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

	При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow9** выбран для основного парсинга, дополнительная нормализация недоступна. В правилах сопоставления по умолчанию для метода парсинга **netflow9** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`. • **sflow5** Этот метод парсинга используется для обработки данных в формате sflow5. При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **sflow5** выбран для основного парсинга, дополнительная нормализация недоступна. • **ipfix** Этот метод парсинга используется для обработки данных в формате IPFIX. При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна. В правилах сопоставления по умолчанию для метода парсинга **ipfix** в полях событий KUMA не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`. • **sql** Нормализатор использует этот метод парсинга для обработки данных, полученных с помощью выборки из базы данных. • **normalizer** Этот метод парсинга позволяет переиспользовать ранее созданный нормализатор в качестве основного или дополнительного для обработки событий. При выборе этого метода парсинга вам нужно в раскрывающемся списке **Нормализатор** выбрать один из ранее созданных нормализаторов с типом json, cef, regexp, syslog, csv, kv, xml или sql. Нормализаторы с методом парсинга **normalizer** недоступны для выбора. Обязательный параметр.
Название	Название правил парсинга. Максимальная длина имени: 128 символов в кодировке Unicode. Название основного правила парсинга будет использоваться в качестве названия нормализатора. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Параметр недоступен для дополнительных правил парсинга.
Сохранить исходное событие	Сохранение исходных событий во вновь созданном нормализованном событии. Доступные значения: • **Не сохранять** – не сохранять исходное событие. Это значение используется по умолчанию. • **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке сервиса, так как в этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок. 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 исходное событие** → **При возникновении ошибок**. • **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события. Обязательный параметр. Параметр недоступен для дополнительных правил парсинга.

Сохранить дополнительные поля	Сохранение поля и значения, для которых не настроены правила сопоставления. Данные сохраняются в поле события `Extra` в виде массива. 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`.
	  Вам нужно указать значение 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. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	
	По умолчанию дополнительные поля не сохраняются.
	Обязательный параметр. Параметр недоступен для метода парсинга **normalizer**.

Описание	Описание ресурса. Максимальная длина описания: до 4000 символов в кодировке Unicode. Параметр недоступен для дополнительных правил парсинга.
Примеры событий	Пример данных, которые вы хотите обработать. Параметр недоступен для методов парсинга **netflow5**, **netflow9**, **sflow5**, **ipfix**, **sql** и **normalizer**. Если парсинг события был выполнен успешно и тип полученных из сырого события данных совпадает с типом поля KUMA, поле **Примеры событий** заполняется данными, полученными из сырого события. 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**.

Сопоставление	Параметры для настройки сопоставления полей исходного события с полями события в формате KUMA:
	• **Исходные данные** – названия полей исходного события, которые вы хотите преобразовать в поля события KUMA.
	Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором вы можете с помощью кнопки **Добавить преобразование** создавать правила для изменения исходных данных перед записью в поля событий KUMA. Вы можете менять местами и удалять созданные правила. Для изменения места правила используйте значок ⠿ рядом с ним. Для удаления правила нажмите рядом с ним на значок ✕.
	Доступные преобразования
	
	Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
	
	• **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
	
	• **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
	
	• **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
	
	  • **Символы на замену** – последовательность символов, которую требуется заменить.
	
	  • **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
	
	• **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
	
	• **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
	
	• **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
	
	• **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
	
	  • **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
	
	  • **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.
	  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.
	
	• Преобразование формата IP-адреса в IPv4:
	
	  • **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
	
	  • **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

- **Поле KUMA** – поля событий KUMA. Вы можете искать поля, вводя их названия.
- **Подпись** – уникальная пользовательская метка полей событий, которые начинаются с `DeviceCustom*` и `Flex*`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить строку**. Для удаления отдельной строки таблицы нажмите рядом с ней на значок ✕. Для удаления всех строк таблицы нажмите на кнопку **Очистить все**.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

Если размер поля события KUMA оказывается меньше длины помещаемого в него значения, значение обрезается до размера поля события.

Эти параметры недоступны для метода парсинга **normalizer**.

Расширенная схема событий

Вы можете использовать поля расширенной схемы событий в нормализаторах для нормализации событий и в других ресурсах KUMA, например, в качестве полей виджетов, а также в SQL-запросах для фильтрации и поиска событий, в таблице событий и пресетах. Список всех полей расширенной схемы событий, существующих в KUMA, доступен в разделе **Параметры** → **Поля расширенной схемы событий**. Список полей расширенной схемы событий единый для всех тенантов.

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 сущностей 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.

- `KL_AI_DLLHijackingCheckResult`, тип `N` – предназначено для хранения информации о результате проверки динамической библиотеки, которая потенциально может использоваться в атаках типа DLL Hijacking. Результат проверки выдает сервис KSN.

- 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". Мы не рекомендуем 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 веб-консоли KUMA в разделе **Параметры** → **Поля расширенной схемы событий** нажмите на кнопку **Добавить** в верхней части таблицы.

   Откроется панель **Создание расширенной схемы**.

2. 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.

3. 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.

4. В поле **Имя** поля укажите имя поля расширенной схемы событий.

   Имя поля расширенной схемы событий имеет следующие особенности:

   - Должно быть уникальным в рамках инсталляции KUMA.
   - 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.

5. При необходимости в поле **Описание** укажите описание поля расширенной схемы событий.

   Мы рекомендуем в описании указывать назначение добавляемого поля расширенной схемы событий. В описании допустимо использовать только символы Unicode. Максимальная длина – 256 символов.

6. 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 веб-консоли KUMA в разделе **Параметры** → **Поля расширенной схемы событий** нажмите на название поля, которое вы хотите 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).

2. 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.

3. 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 инсталляции 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 веб-консоли KUMA в разделе **Параметры** → **Поля расширенной схемы событий** нажмите на кнопку **Импорт**.

2. 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 веб-консоли KUMA перейдите в раздел **Параметры** → **Поля расширенной схемы событий**.

2. 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.

3. 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 сущностях KUMA (нет зависимостей). Мы рекомендуем 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 веб-консоли KUMA перейдите в раздел **Параметры** → **Поля расширенной схемы событий**.

2. 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.

3. 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 и сложности восприятия данных.

Мы рекомендуем 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. Заполните основные параметры нормализатора.
3. Нажмите на кнопку **Добавить строку**.
4. В параметре **Исходные данные** укажите 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`.

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. Правила обогащения хранятся в параметрах нормализатора, в котором они были созданы.

Вы можете создавать правила обогащения с помощью кнопки **Добавить обогащение**. Для удаления правила обогащения нажмите рядом с ним на кнопку ×. Поля расширенной схемы событий могут быть использованы при обогащении событий. Доступные параметры правила обогащения описаны в таблице ниже.

Доступные параметры правила обогащения

Параметр	Описание

Тип источника	Тип обогащения. В зависимости от выбранного типа обогащения отобразятся дополнительные параметры, которые также потребуется заполнить. Доступные типы обогащения:

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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.

- **словарь**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

- **таблица**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

  Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

  Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

  Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события KUMA, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий KUMA, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.
- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` — это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

Обязательный параметр.

Целевое поле	Поле события KUMA, в которое требуется поместить данные. Обязательный параметр. 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 которых события будут поступать на обработку в правило парсинга. Условия можно задать в окне **Дополнительное правило парсинга** 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**. Мы рекомендуем 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**.

  > Параметр **Использовать сырое событие** не работает, если в основном правиле парсинга событий использован метод парсинга sql.

- **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.

  Если при настройке параметров дополнительного нормализатора вы указали для параметра **Использовать сырое событие** значение **Нет** и значение в поле **Исходное поле** осталось незаполненным, любые настроенные преобразования для поля, которое передается в нормализатор, не будут работать. Чтобы преобразования выполнялись корректно, исходное поле должно быть заполнено либо указано значение **Да** для параметра **Использовать сырое событие**.

  KUMA никак не ограничивает и не проверят текст, который вы указываете в этом параметре.

- 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. KUMA никак не ограничивает и не проверят текст, который вы указываете в полях левого и правого операнда.

- 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** – левый операнд соответствует регулярному выражению (RE2), указанному в правом операнде.

- **in** – левый операнд соответствует одному из значений, указанных в правом операнде.

Поступающие данные можно предварительно преобразовать, если нажать на кнопку 🔧: откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно 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 применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

- **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.
- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **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.
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 типов событий, полученных от сетевых коммутаторов Alcatel по Syslog.
Ansible	[OOTB] Ansible syslog	Syslog	Предназначен для обработки событий, поступающих от системы Ansible (версия 2.10.8) по Syslog.
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	Предназначен для обработки событий в журналах СУБД Apache Cassandra версии 4.0.
Apache Kafka	[OOTB] Apache Kafka syslog	regexp	Предназначен для обработки событий аудита системы Apache Kafka версии 3.8.1, поступающих по Syslog.
Apache Tomcat	[OOTB] Apache Tomcat json	Syslog	Предназначен для обработки событий, поступающих от системы Apache Tomcat (версии 9.0 и выше, 10.1 и выше, 11.0 и выше) по Syslog в форматах JSON и key-value.
APC Smart-UPS	[OOTB] APC Smart UPS	regexp	Предназначен для обработки событий аудита системы APC Smart-UPS.
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Atlassian Confluence	[OOTB] Atlassian Jira Conflunce file	regexp	Предназначен для обработки событий систем Atlassian Jira, Atlassian Confluence (Jira версия 9.12, Confluence версия 8.5), хранящихся в файлах.
Atlassian Jira	[OOTB] Atlassian Jira Conflunce 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 версии 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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 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 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.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	Предназначен для обработки событий, поступающих по Syslog от системы Canonical LXD версии 5.18.
Check Point	[OOTB] Checkpoint syslog	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана Check Point версии R81 по 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 ACE	[OOTB] Cisco ASA and IOS syslog	regexp	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco ASA	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	Предназначен для обработки журнала событий прокси-сервера Cisco Email Security Appliance (WSA) версии 14.2, файл access.log.
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	Предназначен для обработки типов событий, полученных от Cisco ESA версии 16.0 по Syslog.
Cisco Firepower Threat Defense	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Firewall Services Module (FWSM)	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	Предназначен для обработки событий системы Cisco Identity Services Engine (ISE) версии 3.2, поступающих по Syslog.
Cisco IOS	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS 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 Next-Generation Intrusion Prevention System (NGIPS)	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco PIX	[OOTB] Cisco ASA and IOS syslog	regexp	Предназначен для обработки типов событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Cisco Wireless LAN Controllers (WLCs)	[OOTB] Cisco WLC syslog	regexp	Предназначен для обработки типов событий, поступающих от сетевых устройств Cisco WLCs (2500 Series Wireless Controllers, 5500 Series Wireless Controllers, 8500 Series Wireless Controllers, Flex 7500 Series Wireless Controllers) по Syslog.
Cisco Web Security Appliance (WSA)	[OOTB] Cisco WSA file, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA file – нормализатор, который 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, который предназначен для обработки событий, поступающих от системы Cisco WSA (версия 15.0) по Syslog.
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	Содержит набор ресурсов для обработки части событий модуля SIP системы CommuniGate Pro версии 6.1 и 6.5.1, передаваемых агентом KUMA по протоколу TCP. Подробнее о настройке коллектора см. Создание коллектора.
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	[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.
Deep Instinct	[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 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
D-Link Switchesr	[OOTB] D-Link Switches	regexp	Предназначен для обработки событий, поступающих от коммутаторов D-Link (DES-2108, DES-3200-28, DES-3828, DES-3800) по Syslog.
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.
EclecticIQ Threat Intelligence Platform	[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] ESET Protect syslog CEF	Syslog	Предназначен для обработки событий, поступающих в формате CEF от системы ESET PROTECT (версия 11.0) по Syslog. Пакет доступен для KUMA версии 3.2 и выше.
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	Предназначен для обработки 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 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.
Flant Deckhouse	[OOTB] Flant Deckhouse json	json	Предназначен для обработки событий аудита уровня Metadata системы Deckhouse (версия 1.67) в формате JSON.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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] FortiGate syslog KV [OOTB] FortiGate syslog CEF	regexp	[OOTB] FortiGate syslog KV – нормализатор, который предназначен для обработки событий, поступающих от межсетевых экранов FortiGate (версии 7.0, 7.2) по syslog. Источник событий – журналы FortiGate в формате key-value. [OOTB] FortiGate syslog CEF – нормализатор, который предназначен для обработки событий, поступающих от системы Fortinet FortiGate (версия FortiOS 6.4) по syslog в формате CEF.
Fortinet FortiMail	[OOTB] Fortimail	regexp	Предназначен для обработки событий системы защиты электронной почты FortiMail. Источник событий – журналы почтовой системы FortiMail.
Fortinet FortiPAM	[OOTB] Fortinet FortiPAM syslog	regexp	Предназначен для обработки событий, поступающих от системы Fortinet FortiPAM (версия 7.4) в формате key-value по протоколу Syslog.
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
FreeIPA	[OOTB] FreeIPA	json	Предназначен для обработки событий, поступающих от системы FreeIPA. Источник событий – журналы службы каталогов FreeIPA.
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 Garda DB	[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.
Grafana	[OOTB] Grafana syslog json	Syslog	Предназначен для обработки событий, поступающих от системы Grafana версии 9.5.15 в формате JSON по Syslog.
HAProxy	[OOTB] HAProxy syslog	Syslog	Предназначен для обработки событий, поступающих от HAProxy версии 2.4 по Syslog. Нормализатор поддерживает обработку событий в форматах Default, TCP, TCP CLF (версии 3.2 и выше), HTTP, HTTP CLF, HTTPS (версии 2.6 и выше) и Error.
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 межсетевых экранов Huawei Eudemon. Источник событий – журналы межсетевых экранов Huawei Eudemon.
Huawei iManager 2000	[OOTB] Huawei iManager 2000 file	regexp	Предназначен для обработки 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	Предназначен для обработки 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 Privileged Access Manager	[OOTB] Indeed PAM syslog [OOTB] Indeed PAM syslog CEF	Syslog	Нормализатор [OOTB] Indeed PAM syslog предназначен для обработки событий, поступающих от системы Indeed Privileged Access Manager версии 2.6. Нормализатор [OOTB] Indeed PAM syslog CEF предназначен для обработки событий, поступающих от системы Indeed Privileged Access Manager (версия 3.3) в формате CEF по Syslog.
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.
IPFIX	[OOTB] IPFIX	ipfix	Предназначен для обработки событий в формате IP Flow Information Export (IPFIX).
Juniper JUNOS	[OOTB] Juniper-JUNOS	regexp	Нормализатор для событий Juniper JUNOS (версия 24.2), поступающих по Syslog.
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 DFI	[OOTB] Kaspersky DFI json	json	Предназначен для обработки событий аудита системы Kaspersky DFI в формате JSON. Нормализатор поддерживает обработку событий, сформированных коннектором KUMA "dfi". Доступен в наборе ресурсов для KUMA версии 4.0 и выше.
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 for 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 for Linux (KESL) версии 12.2 в формате CEF по syslog. [OOTB] KESL json – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Endpoint Security for 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Kaspersky Industrial CyberSecurity for Networks 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	Нормализатор [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog предназначен для обработки событий, поступающих от системы Kaspersky Industrial CyberSecurity for Networks версии 4.2 по Syslog. Этот нормализатор устарел. Рекомендуется использовать нормализатор [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog.
Kaspersky Industrial CyberSecurity for Networks 4.2, 4.3, 4.5	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky Industrial CyberSecurity for Networks версии 4.2, 4.3, 4.5 по Syslog.
Kaspersky IoT Secure Gateway (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.
Kaspersky NDR	[OOTB] Kaspersky NDR syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky NDR версии 7.0 по Syslog. Пакет доступен для KUMA версии 3.2 и выше.
Kaspersky Security Center	[OOTB] KSC	cef	Предназначен для обработки событий Kaspersky Security Center в формате CEF.
Kaspersky Security Center	[OOTB] KSC from SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы Kaspersky Security Center.
Kaspersky Security for 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	Предназначен для обработки событий системы Kaspersky Security for Exchange (KSE) версия 9.0, хранящихся в БД.
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG syslog CEF [OOTB] KSMG 2.1+ syslog CEF	Syslog	[OOTB] KSMG syslog CEF – нормализатор для обработки событий KSMG версии 2.0 в формате CEF по Syslog. [OOTB] KSMG 2.1+ syslog CEF – нормализатор для обработки событий, поступающих от системы KSMG версии 2.1.1, 3.0 в формате CEF по Syslog.
Kaspersky Unified Monitoring and Analysis Platform (KUMA)	[OOTB] KUMA forwarding	json	Предназначен для обработки событий, перенаправленных из Kaspersky Unified Monitoring and Analysis Platform (KUMA).
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF, [OOTB] KWTS (KV)	Syslog	[OOTB] KWTS Syslog CEF – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Web Traffic Security в формате CEF по Syslog. [OOTB] KWTS (KV) – нормализатор, который предназначен для обработки событий Kaspersky Web Traffic Security в формате key-value.
Keycloak	[OOTB] Keycloak syslog	Syslog	Предназначен для обработки событий аудита системы Keycloak версии 26.3, поступающих по Syslog.
Kemp Technologies LoadMaster	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Kerio Control	[OOTB] Kerio Control	Syslog	Предназначен для обработки событий межсетевых экранов Kerio Control.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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. Пакет доступен для KUMA версии 3.2 и выше.
McAfee Web Gateway	[OOTB] McAfee Web Gateway	regexp	Предназначен для обработки событий, поступающих от системы McAfee Web Gateway (версия 7.8 и выше) в форматах CEF и KV по Syslog.
Microsoft Active Directory Certificate Services (AD CS)	[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 Active Directory Certificate Services (AD CS) в формате XML. Нормализатор [OOTB] Microsoft Products for KUMA 3 поддерживает работу с этим источником событий в KUMA 3.0.1 и выше.
Microsoft Active Directory Federation Service (AD FS)	[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 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 [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 Microsoft AD DS. Нормализатор [OOTB] Microsoft Products for KUMA 3 поддерживает работу с данным источником событий в KUMA 3.0.1 и выше.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft Defender	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 системы 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 [OOTB] Microsoft DNS ETW logs json	regexp	Нормализатор [OOTB] DNS Windows предназначен для обработки событий DNS сервера Microsoft. Источник событий – журналы DNS сервера Windows. Нормализатор не поддерживает обработку событий журнала отладки с включенной опцией **Details**. Нормализатор [OOTB] Microsoft DNS ETW logs json предназначен для обработки части событий аудита Microsoft DNS Server, предоставляемых ETW-провайдером. Пакет доступен для KUMA версии 3.2 и выше.
Microsoft Exchange Server	[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 [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 операционной системы 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 Installer	[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 Installer (MSI Installer) в формате XML.
Microsoft IIS	[OOTB] IIS Log File Format	regexp	Предназначен для обработки событий 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 [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 операционной системы Microsoft Windows. Источник событий – события Network Policy Server.
Microsoft Office 365	[OOTB] Microsoft Office 365 json	json	Предназначен для обработки типов событий аудита Microsoft Office 365. Нормализатор поддерживает обработку типов событий аудита, поступающих от систем Microsoft Teams, Azure Active Directory, SharePoint. Пакет доступен для KUMA версии 3.4 и выше.
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	Предназначен для обработки части событий системы Microsoft SharePoint Server (версия SharePoint Server 2016), хранящихся в диагностических журналах.
Microsoft Sysmon	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 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 [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 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft → Windows → AppLocker	[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 → AppLocker в формате XML.
Microsoft → Windows → DNS-Server → Audit	[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 → DNS-Server → Audit в формате XML.
Microsoft → Windows → Group Policy → 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 → Group Policy → Operational в формате XML.
Microsoft → Windows → PowerShell	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 журналов PowerShell операционной системы Microsoft Windows.
Microsoft → Windows → PowerShell-Operational	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft → 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.
Microsoft → 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.
Microsoft → 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 SQL Server, Microsoft SQL Server Express	[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 MS SQL Server версии 2008 и новее.
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 операционной системы 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft Windows Service Control Manager	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [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 журналов Service Control Manager (журнал System) операционной системы Microsoft Windows.
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 [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 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.
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

Название системы	Название нормализатора	Тип	Описание нормализатора
Netgear Switch	[OOTB] Netgear Switch syslog	regexp	Предназначен для обработки событий аудита, поступающих от коммутатора Netgear (модель M4300-52G).
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.
Netwrix Endpoint Protector	[OOTB] Netwrix Endpoint Protector syslog	regexp	Предназначен для обработки событий, поступающих от системы Netwrix Endpoint Protector (версия 5.9) по Syslog. Пакет доступен для KUMA версии 3.2 и выше.
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.
NFS kernel server	[OOTB] NFS kernel server syslog	regexp	Предназначен для обработки событий NFS kernel server (версии NFSv3, NFSv4.0, NFSv4.1, NFSv4.2) в формате Syslog.
Nginx	[OOTB] Nginx regexp	regexp	Предназначен для обработки журнала событий веб-сервера Nginx в формате Combined. Нормализатор поддерживает обработку событий, поступающих по Syslog и хранящихся в файле. Пакет доступен для KUMA версии 3.2 и выше.
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NPO Fractel	[OOTB] NPO Fractel SSPT-4	regexp	Предназначен для обработки событий системы НПО Фрактел ССПТ-4А1.
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.
OpenVPN	[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.
Orion soft Cloudlink	[OOTB] OrionSoft Cloudlink syslog	regexp	Предназначен для обработки событий, поступающих от системы Orion soft Cloudlink (версия 1.0) в формате CEF по Syslog.
Orion soft Termit	[OOTB] OrionSoft Termit syslog	Syslog	Предназначен для обработки событий, поступающих от системы Orion soft 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 zVirt 3.1, 4.4, 4.5, 5.0 и zVirt Max 1.2).
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] Palo Alto NGFW syslog csv	Syslog	Предназначен для обработки событий от межсетевых 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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.
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 Multiscanner	[OOTB] PTsecurity Multiscanner json	Syslog	Предназначен для обработки событий, поступающих от системы PT Multiscanner (версия 5.24) формате JSON по Syslog.
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	Предназначен для обработки событий системы PT Sandbox.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF syslog	Syslog	Предназначен для обработки событий, поступающих от системы PTsecurity Web Application Firewall версии 4 по Syslog.
Postfix	[OOTB] Postfix syslog	regexp	Содержит набор ресурсов для обработки событий Postfix версии 3.6. Поддерживается обработка Syslog-событий, поступающих по протоколу TCP. Пакет доступен для KUMA 3.0 и более новых версий.
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 системы Proftpd версии 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 версии 2.6, хранящихся в файле.
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	Предназначен для обработки журналов системы RedCheck WEB версии 2.6, хранящихся в файлах.

Название системы	Название нормализатора	Тип	Описание нормализатора
RED SOFT RED ADM	[OOTB] RED SOFT RED ADM syslog	regexp	Предназначен для обработки событий, поступающих от системы RED ADM (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 межсетевого экрана pfSense, поступающих по Syslog.
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана pfSense. Syslog-заголовок этих событий не содержит имени хоста.
RuPost LLC WorksPad	[OOTB] RuPost LLC WorksPad CEF syslog	Syslog	Предназначен для обработки части событий системы RuPost LLC WorksPad (версия 6.3.70) в формате CEF, поступающих по Syslog.
SafeTech CA SQL	[OOTB] SafeTech CA SQL	sql	Предназначен для обработки событий, поступающих из СУБД PostgreSQL системы SafeTech CA версии 3.2.
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
SaltStack	[OOTB] SaltStack syslog	Syslog	Предназначен для обработки однострочных событий, поступающих от системы SaltStack (версия 3004.1 и старше) по Syslog. Нормализатор не поддерживает обработку многострочных событий.
SecurityCode Continent 3.9	[OOTB] SecurityCode Continent 3.9 json	json	Предназначен для обработки событий системы SecurityCode Continent версии 3.9.2, поступающих от утилиты kuma-kont в формате json. Пакет доступен для KUMA версии 3.4 и выше.
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.
Seqrite EPS	[OOTB] Seqrite EPS CEF	cef	Предназначен для обработки событий, поступающих от системы Seqrite EPS версии 6.0 в формате CEF.
Skype for Business	[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 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	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана Sonicwall TZ в формате key-value (версия 7.3), в формате CEF (версия 6.5, 7.3) по Syslog.
Solar webProxy	[OOTB] Solar WebProxy syslog	regexp	Предназначен для обработки событий, поступающих от Solar webProxy версии 4.2 в формате siem-log по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
SolarWinds DameWare MRC	[OOTB] SolarWinds DameWare MRC xml	xml	Предназначен для обработки части событий системы DameWare Mini Remote Control (MRC) версия 7.5, хранящихся в журнале Application операционной системы Windows. Нормализатор обрабатывает события, создаваемые провайдером dwmrcs.
SolarWinds SFTP & SCP Server file	[OOTB] SolarWinds SFTP & SCP Server file	regexp	Предназначен для обработки журнала событий SolarWinds SFTP & SCP Server (версия 2.2), хранящегося в файле SftpServer.log. Пакет доступен для KUMA версии 3.2 и выше.
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 межсетевого 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	Предназначен для обработки 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.
Synesis The Wall WAF	[OOTB] Synesis The Wall WAF syslog	Syslog	Предназначен для обработки событий Synesis TheWall WAF, поступающих по Syslog.
TeamPass	[OOTB] TeamPass SQL	sql	Предназначен для обработки событий, поступающих от системы TeamPass (версия 3.1), хранящихся в базе данных.
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.
Tionix VDI	[OOTB] Tionix VDI file	regexp	Предназначен для обработки 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.
Umbraco CMS	[OOTB] Umbraco CMS syslog	regexp	Предназначен для обработки событий системы Umbraco CMS версии 11.4.1 в формате Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
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.
Veeam Software – Veeam Backup & Replication	[OOTB] Veeam Software Veeam Backup & Replication syslog	regexp	Предназначен для обработки событий, поступающих от системы Veeam Software – Veeam Backup & Replication версии 12.1 по Syslog.
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.
VK Private Cloud	[OOTB] VK Private Cloud syslog	regexp	Предназначен для обработки событий аудита VK Private Cloud (версия 1.0), поступающих по Syslog.
VK WorkSpace Mail	[OOTB] VK WorkSpace Mail syslog	Syslog	Предназначен для обработки событий, поступающих от системы VK WorkSpace Mail версии 1.23 по Syslog в формате key-value.
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	Syslog	Предназначен для обработки событий межсетевых экранов WatchGuard Firebox (версия OS v2026.1.B730198), поступающих по Syslog.
Webmonitorx	[OOTB] Webmonitorx json	regexp	Предназначен для обработки событий, поступающих от системы Webmonitorx в формате JSON.
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Windchill FRACAS	[OOTB] PTC Winchill Fracas	regexp	Предназначен для обработки событий системы регистрации сбоев Windchill FRACAS.
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), Backup.
Zabbix	[OOTB] Zabbix SQL	sql	Предназначен для обработки событий Zabbix версии 6.4.
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	Предназначен для обработки части событий системы Zecurion DLP версии 13.0, поступающих в формате CEF по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
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 – Синоникс	[OOTB] Bastion Synonyx CEF	regexp	Предназначен для обработки событий в формате CEF, поступающих от системы АйТи Бастион – Синоникс версии 1.7. Пакет с нормализатором доступен для KUMA версии 3.2 и выше.
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 Angie	[OOTB] Angie syslog	Syslog	Предназначен для обработки событий, поступающих от системы Angie и Angie Pro (версия 1.10.1) по Syslog. Пакет с нормализатором доступен для KUMA версии 3.2 и выше.
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 событий 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 [OOTB] VipNet Coordinator CEF	Syslog	Нормализатор [OOTB] VipNet Coordinator Syslog предназначен для обработки событий от системы ИнфоТеКС ViPNet Coordinator, поступающих по Syslog. Нормализатор [OOTB] VipNet Coordinator CEF предназначен для обработки событий, поступающих от системы ИнфоТеКС ViPNet Coordinator (версии 4.5) в формате CEF.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Конфидент - Единый центр управления Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Предназначен для обработки событий, поступающих от систем: Dallas Lock 8 (версия 11.4.2.843, 12.10.6.877), Единый центр управления (ЕЦУ) Dallas Lock (версия 4.0.294.0, 4.0.354.0) в формате CEF.
Конфидент - Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Предназначен для обработки событий, поступающих от системы Dallas Lock 8 (версия 11.4.2) в формате CEF.
КриптоПро NGate	[OOTB] Ngate Syslog	Syslog	Предназначен для обработки событий, поступающих от системы КриптоПро NGate по Syslog.
Маршрутизаторы H3C (Huawei-3Com)	[OOTB] H3C Routers syslog	regexp	Предназначен для обработки типов событий, поступающих от сетевых устройств H3C (Huawei-3Com) SR6600 (прошивка Comware 7) по Syslog. Нормализатор поддерживает формат событий standard (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	Syslog	Нормализатор для обработки событий системы СКДПУ НТ Шлюз доступа версии 7.0 (сборка17, обновление 14) и 7.1.1, 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.
Яндекс 360	[OOTB] Yandex 360 json	json	Предназначен для обработки событий, поступающих от системы Яндекс 360 в формате JSON. Транспорт для получения событий будет доступен в KUMA версии 4.2.
Яндекс Браузер корпоративный	[OOTB] Yandex Browser	json	Предназначен для обработки событий, поступающих от корпоративной версии Яндекс Браузера версии 23, 24.4, 25.2.
-	[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 вы можете уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор, снизить нагрузку на сервисы, 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.

Вы можете настроить правила агрегации в разделе **Ресурсы** → **Правила агрегации**, а затем выбрать созданное правило агрегации в раскрывающемся списке в параметрах коллектора. Правила агрегации также можно настроить напрямую в параметрах коллектора. Доступные параметры правила агрегации описаны в таблице ниже.

Вкладка Общие

Вкладка Общие

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени: до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
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. Значение по умолчанию: `100`.
Время ожидания событий	Ограничение по времени в секундах. По истечении указанного срока накопление базовых событий прекращается, коллектор создает агрегированное событие и начинает сбор событий для следующего агрегированного события. Значение по умолчанию: `60`. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания: 4000 символов в кодировке Unicode.
Группирующие поля	Поля нормализованных событий, значения которых должны совпадать. Например, для сетевых событий могут использоваться поля нормализованных событий `SourceAddress`, `DestinationAddress` и `DestinationPort`. В итоговом агрегационном событии поля нормализованных событий будут заполнены значениями базовых событий. Обязательный параметр.
Уникальные поля	Поля нормализованных событий, значения которых должны быть уникальными для того, чтобы эти события учитывались в агрегированном событии. Если значение поля, указанного в **Уникальные поля**, дублируется в нескольких событиях, только одно из таких событий попадет в агрегированное событие, а повторы будут проигнорированы. Если в **Уникальные поля** вы укажете более одного поля, то уникальными должны быть сочетания значений всех этих полей. Уникальные поля не сохраняются в агрегированном событии.
Поля суммы	Поля, значения которых при агрегации будут просуммированы и записаны в одноименные поля агрегированного события. Существуют следующие особенности поведения полей: • значения полей с типами `Число` и `Число с плавающей точкой` суммируются; • значения полей с типом `Строка` конкатенируются через запятую; • значения полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` добавляются в конец массива.

Параметр	Описание
Фильтр	Условия определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать в раскрывающемся списке существующий фильтр или **Создать**, чтобы создать новый 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 сервиса. Для этого нужно установить флажок рядом с нужным коллектором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Предустановленные правила агрегации

В поставку KUMA включено правило агрегации **[OOTB] Netflow 9**. Правило сработает при достижении 100 событий или по истечении 10 секунд.

Агрегация событий выполняется по следующим полям:

- `DestinationAddress`
- `DestinationPort`
- `SourceAddress`
- `TransportProtocol`
- `DeviceVendor`
- `DeviceProduct`

Поля `DeviceCustomString1` и `BytesIn` суммируются.

https://rutube.ru/video/37e0e77d1ec1d71a321d29a25c654201/

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. В коллекторе можно создать правило обогащения и оно станет ресурсом, доступным для переиспользования в других сервисах. Также можно привязать правило обогащения, созданное как отдельный ресурс.
- Коррелятор. В корреляторе можно создать правило обогащения и оно станет ресурсом, доступным для переиспользования в других сервисах. Также можно привязать правило обогащения, созданное как отдельный ресурс.
- Нормализатор. В нормализаторе можно только создать правило обогащения, которое будет привязано только к нормализатору и не будет доступно как отдельный ресурс для использования в других сервисах.

Доступные параметры правил обогащения перечислены в таблице ниже.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила обогащения (см. таблицу ниже).

Вкладка Общие

Параметр	Описание

Тип источника данных	Обязательный параметр. Раскрывающийся список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры:

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

- **таблица**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

  Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

  Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

  Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **обогащение активами**

  Этот тип обогащения используется, когда необходимо добавить обогащение событий активами на определенных коллекторах.

  Для обогащения событий активами в блоке **Сопоставление** необходимо заполнить таблицу сопоставления полей события KUMA и полей для записи значениий из хеш-таблицы:

  1. Нажмите на кнопку **Добавить**.
  2. В раскрывающемся списке **Поле KUMA** выберите одно или несколько полей события, значение которого будет сопоставляться со значением из хеш-таблицы и записываться в соответствующее поле в таблице для записи данных актива.
  3. В раскрывающемся списке **Поле для записи данных** выберите поле, в которое, в случае соответствия поля события (**Поле KUMA**) и значения из хеш-таблицы, будет записано значение идентификатора актива.

     Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных
DestinationAddress DestinationHostName DeviceAddress DeviceHostName SourceAddress SourceHostName DestinationMacAddress DeviceMacAddress SourceMacAddress DeviceCustomString1 DeviceCustomString2 DeviceCustomString3 DeviceCustomString4 DeviceCustomString5 DeviceCustomString6	SourceAssetID DeviceAssetID DestinationAssetID

Если пользователь выбирает несколько полей, к значениям полей применяется условие **И**. Если пользователь добавляет несколько строк в столбце **Поле KUMA**, к значениям полей применяется условие **ИЛИ**. Проверка начинается с первого поля в списке. Если значение поля совпадает со значением атрибута, проверка прекращается.

Например, в событие поступают следующие данные:

```
SourceAddress=192.168.x.xx
SourceHostName=kuma.example.com.
```

В KUMA есть два актива: *company.example.com* (IP-адрес: 192.168.x.xx, FQDN: company.example.com) и *kuma.example.com* (IP-адрес: 192.168.y.yyy, FQDN: kuma.example.com). Сопоставление для них осуществляется следующим образом:

- Если пользователь указал отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (company.example.com).
- Если пользователю важнее получить значение параметра `sourceHostname` (kuma.example.com), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.
- Если пользователь указал `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

В таблице сопоставления полей должно быть указано хотя бы одно условие сопоставления.

Вы также можете нажать на кнопку **Применить сопоставление по умолчанию**, расположенную над таблицей. В этом случае будут применены значения параметров **Поле KUMA** и **Поле для записи данных**.

Установленные по умолчанию значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных
DestinationAddress	DestinationAssetID
DestinationHostName	DestinationAssetID
DeviceAddress	DeviceAssetID
DeviceHostName	DeviceAssetID
SourceAddress	SourceAssetID
SourceHostName	SourceAssetID

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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.

- **словарь**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['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 применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
    - **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
    - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
    - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
      - **Символы на замену** – последовательность символов, которую требуется заменить.
      - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
    - **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
    - **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
    - **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
    - **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
      - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
      - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

- **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.

  Доступные параметры:

  - **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
  - **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.
  - **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Срок жизни кеша** – время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
  - **Кеш отключен** – с помощью этого переключателя можно включить или отключить кеширование. По умолчанию кеширование включено.
  - **Обновление кеша 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 доступен начиная с KUMA 3.4.1. С помощью переключателя можно включить отправку коллектором KUMA рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace**

  > Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения cybertrace-http. Этот тип возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.

  > При обогащении через cybertrace коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в CyberTrace содержит квадратные скобки, например **[str1**, **str2]**), KUMA обрабатывает его как массив, а не как строку.

  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. Порт CyberTrace по умолчанию 9999.
- **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. Значение по умолчанию: `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
- **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000.
- **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. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- **cybertrace-http**

  Это новый тип потокового обогащения событий в CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять в системах с большим потоком событий. Производительность cybertrace-http превосходит показатели типа cybertrace.

  Ограничения:

  - Тип обогащения cybertrace-http неприменим для ретроспективного сканирования в KUMA.
  - В случае использования типа обогащения cybertrace-http обнаружения киберугроз не сохраняются в истории CyberTrace в окне Detections.

  Доступные параметры:

  - **Название** (обязательно) – уникальное название правила обогащения. Максимум 128 символов в кодировке Unicode.
  - **Тенант** (обязательно) – имя тенанта, в рамках которого вы планируете вести работу с CyberTrace.
  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443.
  - **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения.
  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
  - **Ключевые поля** (обязательно) – список полей событий, используемых для обогащения событий данными из CyberTrace.
  - **Максимальное кол-во событий в очереди обогащения** – максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: 1 000 000. По достижении 1 млн получаемых событий от сервера CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
  - **Основная версия CyberTrace** – выбор версии 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**.
  - **Отладка** – переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
  - **Теги** – теги для поиска ресурса.

- **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 сервиса, использующего 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 установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис 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**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

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.

- **проверка DLL Hijacking**

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак KUMA использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения KUMA отправляет запрос с информацией из полей события в KSN. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или корреляторе.

> 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** → **Обнаружение атак DLL Hijacking**).

Доступные параметры:

- **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.

- **Максимальный размер кеша** – максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`.

  Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если KUMA отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.

- **Максимальное количество событий в очереди обогащения** – при превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

- **Выполнять повторный запрос** – в ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса. Если этот параметр включен, настройте дополнительные параметры:

  - **Создавать дубликаты событий** – если этот параметр включен, KUMA создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.

    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.

    - Превышено значение, указанное в параметре **Количество запросов**.

    Если этот параметр выключен, KUMA продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:

    - Из KSN получено заключение, отличное от **В обработке**.

    - Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.

    - Превышено значение, указанное в параметре **Количество запросов**.

  - **Количество запросов** – максимальное количество запросов в KSN. Если за указанное число запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.

  - **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.

  - **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

- **Прокси-сервер** – параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.

- **Сопоставление** – таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и списком соответствующих полей событий KUMA. Список параметров в запросе:

  - **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: OldFileHash.

  - **Путь до файла DLL** – полный путь, включающий имя файла; рекомендованное поле для сопоставления: OldFilePath. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

    Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

    Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

  - **Хеш процесса (md5)** – рекомендованное поле для сопоставления: FileHash.

  - **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, KUMA передает этот параметр в KSN в обезличенном виде. Например:

    Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll`

    Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username`

  - **Имя файла DLL** – рекомендованное поле для сопоставления: OldFileName.

  - **Имя процесса** – рекомендованное поле для сопоставления: FileName.

  - **Подпись процесса** – необязательный параметр; рекомендованное поле для сопоставления: FileID. В этом поле нужно указать поле KUMA, которое передает Organization из Subject подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.

  - **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**.

	Для каждого параметра укажите в таблице соответствующее ему поле события KUMA.
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
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 в кодировке Unicode.

Фильтр	Блок параметров, в котором 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 ↗.

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 отвязать правило обогащения от сервиса. Для этого нужно установить флажок рядом с нужным коррелятором или коллектором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Предустановленные правила обогащения

В поставку KUMA включено правило обогащения [OOTB] KATA alert. Это правило используется для обогащения событий, поступивших от KATA в виде гиперссылки на алерт. Гиперссылка размещается в поле **DeviceExternalId**.

Для того чтобы параметр **DeviceExternalID** отображался в виде ссылки в свойствах событий, убедитесь, что в поле **Шаблон** для параметра `DeviceAddress` указаны URL или полное доменное имя, после которых присутствует символ "/", например: `https://example.com:8443/` или `https://example.com/`.

Настройка параметров обогащения коллекторов активами

Если обогащение активами осуществляется на каждом коллекторе, в каждый коллектор направляются данные об активах (UUID, IP-адрес, FQDN). Это может существенно затруднить и замедлить обработку данных в коллекторах.

Вы можете настроить параметры обогащения коллекторов данными активов только на тех коллекторах, на которых это необходимо.

Чтобы создать правило обогащения коллектора активами:

1. Перейдите в раздел **Ресурсы** веб-интерфейса KUMA.

   В правой части раздела **Ресурсы** отобразится таблица с созданными правилами обогащения.

2. В списке тенантов в левой части окна выберите тенант, которому принадлежит ресурс.

3. Нажмите на кнопку **Создать**, расположенную над таблицей.

4. В открывшейся боковой панели укажите значения следующих параметров:

   a. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится это правило обогащения.

   c. В раскрывающемся списке **Исходный тип** выберите **обогащение активами**.

   d. При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.

   e. При необходимости в раскрывающемся списке **Теги** выберите теги для правила обогащения.

   f. При необходимости в поле **Описание** добавьте описание правила обогащения. Описание правила может содержать до 4000 символов в кодировке Unicode.

5. В блоке **Сопоставление** заполните таблицу сопоставления полей следующим образом:

   a. Нажмите на кнопку **Добавить**.

   b. В раскрывающемся списке **Поле KUMA** выберите одно или несколько полей события, значение которого будет сопоставляться со значением из хеш-таблицы и записываться в соответствующее поле в таблице для записи данных актива.

   c. В раскрывающемся списке **Поле для записи данных** выберите поле, в которое, в случае соответствия поля события (**Поле KUMA**) и значения из хеш-таблицы, будет записано значение идентификатора актива.

Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

Если пользователь выбирает несколько полей, к значениям полей применяется условие **И**. Если пользователь добавляет несколько строк в столбце **Поле KUMA**, к значениям полей применяется условие **ИЛИ**. Проверка начинается с первого поля в списке. Если значение поля совпадает со значением атрибута, проверка прекращается.

Например, в событие поступают следующие данные:

```
SourceAddress=192.168.x.xx
SourceHostName=kuma.example.com.
```

В KUMA есть два актива: *company.example.com* (IP-адрес: 192.168.x.xx, FQDN: company.example.com) и *kuma.example.com* (IP-адрес: 192.168.y.yyy, FQDN: kuma.example.com). Сопоставление для них осуществляется следующим образом:

- Если пользователь указал отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (company.example.com).
- Если пользователю важнее получить значение параметра `sourceHostname` (kuma.example.com), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.
- Если пользователь указал `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

> В таблице сопоставления полей должно быть указано хотя бы одно условие сопоставления.

Вы также можете нажать на кнопку **Применить сопоставление по умолчанию**, расположенную над таблицей. В этом случае будут применены значения параметров **Поле KUMA** и **Поле для записи данных**.

Установленные по умолчанию значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных
`DestinationAddress`	`DestinationAssetID`
`DestinationHostName`	`DestinationAssetID`
`DeviceAddress`	`DeviceAssetID`
`DeviceHostName`	`DeviceAssetID`
`SourceAddress`	`SourceAssetID`
`SourceHostName`	`SourceAssetID`

6. В блоке **Параметры фильтра** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке **Фильтр** можно выбрать существующий фильтр или создать новый фильтр.

   Добавление условий и группы условий для фильтра

   Чтобы добавить условия и группы условий для фильтра:

   1. При создании правила обогащения убедитесь, что в блоке **Параметра фильтра** выбрано **Конструктор**.
   2. Нажмите на кнопку **Добавить условие** и в последовательно появляющихся раскрывающихся списках выберите значения событий и оператор фильтра.

      Вы можете добавить несколько условий для фильтра.
   3. При необходимости нажмите на кнопку **Добавить группу**, чтобы добавить группу условий для фильтра.

      Вы можете добавить несколько групп условий.
   4. Нажмите на название логического оператора (**И**, **ИЛИ**, **НЕ**). По умолчанию выбрано значение **И**.

7. Нажмите **Создать**.

Применение правила обогащения при изменении параметров коллектора

Вы можете добавить одно или несколько правил обогащения активами в уже существующий коллектор, изменив его параметры.

Чтобы добавить правило обогащения коллектора активами в параметры коллектора:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коллекторы** и выберите нужный тенант.
2. Нажмите на название коллектора в таблице с созданными коллекторами.
3. В левой части открывшейся боковой панели выберите раздел **Обогащение событий**.
4. Нажмите на кнопку **Добавить обогащение**.
5. В раскрывающемся списке **Правило обогащения** выберите нужное правило обогащения коллектора активами.

   Вы также можете создать правило обогащения коллектора активами, нажав **Создать** в раскрывающемся списке **Правило обогащения**.
6. При необходимости добавьте другое правило обогащения активами, нажав на кнопку **Добавить обогащение**.

   > Добавить одно и тоже правило обогащения повторно невозможно.
7. Нажмите **Сохранить**.

   Добавленное правило обогащения будет применяться KUMA при получении и обработке коллектором сообщений из источников событий.

Правила сбора и анализа данных

Правила сбора и анализа данных используются для обнаружения инцидентов путем анализа событий, сохраненных в базе данных KUMA.

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.

Доступные параметры правила сбора и анализа данных

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
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`
	Вы также можете использовать наборы SQL-функци `enrich` и `lookup`.

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 **Добавить 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 **Добавить 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 **Ресурсы**→**Ресурсы и сервисы**→**Правила сбора и анализа данных**.
- В разделе **События**.

*Чтобы создать правило сбора и анализа данных в разделе **События**:*

1. Создайте или сформируйте SQL-запрос и нажмите на кнопку .

   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 запуска запроса**.

3. Сохраните параметры.

Правило сбора и анализа данных сохранено и доступно в разделе **Ресурсы и сервисы**→**Правила сбора и анализа данных**. Чтобы правило сбора и анализа данных выполнялось, вам нужно создать для него планировщик.

Настройка планировщика для правила сбора и анализа данных

Чтобы правило сбора и анализа данных выполнялось, вам нужно создать для него планировщик.

Планировщик направляет SQL-запросы в заданные вами разделы хранилища с интервалом и глубиной поиска, который вы настраиваете в правиле, а затем преобразует результаты SQL-запросов в базовые события и направляет в коррелятор.

Результаты SQL-запросов, преобразованные в базовые события, не попадают в хранилище.

Для корректной работы планировщика необходимо настроить связь между правилом сбора и анализа данных, хранилищем и корреляторами в разделе **Ресурсы** → **Сбор и анализ данных**.

Для работы с разделом вам нужно иметь одну из следующих ролей: Главный администратор, Администратор тенанта, Аналитик второго уровня, Чтение общих ресурсов, Редактирование общих ресурсов.

Планировщики расположены в таблице по дате последнего запуска. Вы можете сортировать данные в столбцах по возрастанию и убыванию, нажав на значок стрелки вниз (⌄) в заголовке столбца.

Доступные столбцы таблицы планировщиков:

- **Название правила** – название правила сбора и анализа данных, для которого вы создали планировщик.
- **Название тенанта** – название тенанта, которому принадлежит правило сбора и анализа данных.

- **Состояние** – статус планировщика. Возможны следующие значения:
  - **Включено** – планировщик выполняется, правило сбора и анализа данных будет запускаться по заданному расписанию.
  - **Выключено** – планировщик не выполняется.

    Этот статус планировщик имеет по умолчанию при создании. Чтобы планировщик выполнялся, необходимо перевести его в состояние **Включено**.
- **Планировщик завершил работу в** – время последнего запуска правила сбора и анализа данных, для которого вы создали планировщик.
- **Статус выполнения правила** – статус, с которым планировщик завершил работу. Возможны следующие значения:
  - **Ok** – планировщик завершил работу без ошибок, правило выполнено.
  - **Неизвестно** – планировщик переведен в состояние **Включено**, и его статус в данный момент неизвестен. Статус **Неизвестно** отображается, если вы привязали хранилища и корреляторы на соответствующих вкладках и перевели планировщик в состояние **Включено**, но еще не запустили.
  - **Остановлен** – планировщик остановлен, правило не выполняется.
  - **Ошибка** – планировщик завершил работу, правило выполнено с ошибкой.
- **Последняя ошибка** – ошибки (при наличии), которые возникли при выполнении правила сбора и анализа данных.

> Неуспешная попытка отправки событий в установленный коррелятор не является ошибкой.

На панели инструментов в верхней части таблицы вы можете **выполнять действия над планировщиками**.

- Добавить новый планировщик. Нажмите на кнопку **Добавить** и в отобразившемся окне установите флажки рядом с названиями правил сбора и анализа данных, для которых вы хотите создать планировщик.

  > В этом окне вы можете выбрать правило сбора и анализа данных только из ранее созданных. Создать новое правило нельзя.

- Удалить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите удалить, и нажмите на кнопку **Удалить**. Планировщик и привязки удаляются. Правило сбора и анализа данных не удаляется.
- Включить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите включить, и нажмите на кнопку **Включить по расписанию**. Правило сбора и анализа данных, для которого был создан этот планировщик, будет выполняться согласно расписанию, заданному в настройках этого правила.

- Отключить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите отключить, и нажмите на кнопку **Отключить**. Правило сбора и анализа данных временно перестает выполняться, при этом сам планировщик и привязки не удаляются.

- Запустить планировщик. В таблице планировщиков установите флажки рядом с включенными планировщиками, и нажмите на кнопку **Запустить сейчас**. Правило сбора и анализа данных, для которого был создан этот планировщик, выполнится немедленно.

Чтобы изменить параметры планировщика, нажмите на соответствующую строку в таблице.

Доступные параметры планировщика для правил сбора и анализа данных описаны ниже.

Вкладка Общие

На этой вкладке вы можете выполнить следующие действия:

- Включить или выключить планировщик с помощью переключателя.

  Если переключатель включен, правило сбора и анализа данных будет запускаться по расписанию, заданному в его настройках.

- Изменить следующие параметры правила сбора и анализа данных:

  - Название
  - Частота запуска запроса
  - Глубина
  - Sql
  - Описание
  - Сопоставление

Вкладка Привязанные хранилища

На этой вкладке вам нужно задать хранилище, в которое планировщик будет направлять SQL-запросы.

Чтобы задать хранилище:

1. Нажмите на кнопку **Привязать** на панели инструментов.
2. В открывшемся окне укажите название хранилища, к которому вы хотите добавить привязку, а также название раздела выбранного хранилища.

   Вы можете выбрать только одно хранилище, но несколько разделов этого хранилища.

3. Нажмите на кнопку **Добавить**.

   Привязка создана и отображается в таблице на вкладке **Привязанные хранилища**.

При необходимости вы можете удалить привязки, установив флажки в соответствующих строках таблицы и нажав на кнопку **Отвязать выбранные**.

Вкладка Привязанные корреляторы

На этой вкладке вам нужно добавить корреляторы для работы с базовыми событиями.

Чтобы добавить коррелятор:

1. Нажмите на кнопку **Привязать** на панели инструментов.
2. В открывшемся окне установите курсор мыши в поле **Коррелятор**.
3. В отобразившемся списке корреляторов установите флажки рядом с корреляторами, которые вы хотите добавить.
4. Нажмите на кнопку **Добавить**.

   Корреляторы добавлены и отображаются в таблице на вкладке **Привязанные корреляторы**.

При необходимости вы можете удалить корреляторы, установив флажки в соответствующих строках таблицы и нажав на кнопку **Отвязать выбранные**.

Также вы можете просмотреть результат работы планировщика в журнале Ядра, предварительно настроив режим **Отладка** в параметрах Ядра. Чтобы скачать журнал, выберите раздел KUMA **Ресурсы** → **Активные сервисы**, затем выберите сервис Ядра и нажмите на кнопку **Журнал.**

Записи с результатом работы планировщика имеют приставку `datamining scheduler`.

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 его через веб-интерфейс KUMA 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.

Если в правиле корреляции используется другой ресурс, например, сохраненный ранее фильтр, и этот ресурс изменяется, то при экспорте правила корреляции в файл могут попасть данные из более ранней версии измененного ресурса. При этом дальнейший импорт правила корреляции из этого файла завершается корректно, KUMA импортирует последнюю версию ресурса.

https://rutube.ru/video/a37c939ed992377b38a592503ef4d983/

https://rutube.ru/video/cc57b965e06574165617b37ea1d8ac96/

Правило корреляции, тип standard

Правила корреляции с типом **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`.

По сравнению с моделью данных нормализованного события некоторые поля корреляционного события, образованного по правилу корреляции **standard**, могут отличаться (см. таблицу ниже).

Название поля корреляционного события	Описание
StartTime	Самая ранняя дата и время создания базового события (timestamp) среди всех базовых событий, от которых было образовано корреляционное событие.
EndTime	Более поздняя дата и время из следующих: • Дата и время создания корреляционного события. • Самая поздняя дата и время создания базового события (timestamp) среди всех базовых событий, от которых было образовано корреляционное событие.

Чтобы добавить в корреляционное событие поля из базовых событий, укажите эти поля в параметрах **Группирующие поля** и **Уникальные поля** (см.таблицу ниже).

Доступные параметры правила корреляции с типом **standard** описаны в таблицах ниже.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

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.
Тип	Тип правила корреляции – **standard**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Группирующие поля	Поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей событий используется в качестве ключа контейнера. Если срабатывает один из селекторов, указанных на вкладке **Селекторы**, отобранные поля событий копируются в корреляционное событие. Если в разных селекторах корреляционного правила используются поля событий, которые имеют разные значения в событиях, вам не нужно указывать эти поля событий в раскрывающемся списке **Группирующие поля**. Вы можете указывать локальные переменные. Для обращения к локальной переменной вам нужно указать перед ее именем символ `$`. Для ознакомления с примерами использования локальных переменных используйте правило **R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой**, поставляемое с KUMA. Обязательный параметр.
Время жизни контейнера, сек.	Время жизни контейнера в секундах. Отсчет времени начинается при создании контейнера, когда контейнер получает первое событие. По истечении времени жизни контейнера срабатывает триггер, указанный на вкладке **Действия** → **По истечении времени жизни контейнера**, и контейнер удаляется. Триггеры, указанные на вкладках **Действия** → **На каждом срабатывании правила** и **На последующих срабатываниях правила**, могут срабатывать более одного раза в течение времени жизни контейнера. Обязательный параметр.
Уникальные поля	Уникальные поля событий, которые требуется отправлять в контейнер. Если вы указываете уникальные поля событий, только они будут отправляться в контейнер. Хеш-код значений отобранных полей событий используется в качестве ключа контейнера. Вы можете указывать локальные переменные. Для обращения к локальной переменной вам нужно указать перед ее именем символ `$`. Для ознакомления с примерами использования локальных переменных используйте правило **R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой**, поставляемое с KUMA.
Частота срабатываний	Максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: `0`. Если не срабатывают правила корреляции, в которых реализована сложная логика обнаружения закономерностей, причиной могут быть особенности подсчета срабатываний правила в KUMA. В этом случае мы рекомендуем увеличить значение в поле **Частота срабатываний**, например до `1000000`.
Политика хранения базовых событий	Раскрывающийся список, позволяющий определить, какие базовые события требуется поместить в корреляционное событие: • **first** – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события. Это значение выбрано по умолчанию. • **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.
Уровень важности	Базовый коэффициент, используемый для определения уровня важности правила корреляции: • **Критический**. • **Высокий**. • **Средний**. • **Низкий** – это значение выбрано по умолчанию.
Сортировать по	Поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, например если вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Параметр	Описание
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.
Использовать сопоставление уникальных полей	Переключатель, позволяющий сохранять значения уникальных полей в массив и передавать его в одно из полей корреляционного события. Если переключатель включен, в нижней части вкладки **Общие** отображается дополнительный блок параметров **Сопоставление уникальных полей** для настройки сопоставления исходных уникальных полей с полями корреляционного события. При обработке события через правило корреляции сначала выполняется сопоставление полей, затем к уже сформированному на основе сопоставления корреляционному событию будут применены операции, указанные на вкладке **Действия**. По умолчанию переключатель выключен. Необязательный параметр.

Блок параметров Сопоставление уникальных полей

Если необходимо передавать в корреляционное событие значения полей, указанных в параметре **Уникальные поля**, то этот блок можно использовать для настройки сопоставления уникальных полей с полями корреляционного события. Блок отображается на вкладке **Общие**, если включен переключатель **Использовать сопоставление уникальных полей**. Поскольку значения уникальных полей представляют собой массив, поле в корреляционном событии должно иметь соответствующий тип – SA, NA, FA.

Вы можете добавить сопоставление, нажав на кнопку **Добавить** и выбрав в раскрывающемся списке в столбце **Поле исходного события** нужное поле. Для выбора доступны поля, указанные в параметре **Уникальные поля**. В раскрывающемся списке в столбце **Поле события назначения** вам нужно выбрать поле корреляционного события, в которое должен записываться массив значений исходного поля. Для выбора доступны поля, тип которых соответствует массиву (SA, NA или FA в зависимости от типа исходного поля).

Вы можете удалить одно или несколько сопоставлений, установив флажки рядом с нужными сопоставлениями и нажав на кнопку **Удалить**.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для добавления селектора нажмите на кнопку **+ Добавить селектор**. Вы можете добавить несколько селекторов, изменить порядок селекторов и удалить селекторы. Для изменения порядка селекторов используйте значки изменения порядка ⠿. Для удаления селектора нажмите рядом с ним на значок удаления ✕.

Для каждого селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Порог срабатывания селектора (количество событий)	Количество событий, которые требуется получить для срабатывания селектора. Значение по умолчанию: `1`. Обязательный параметр.

Обнуление	Переключатель, позволяющий правилу корреляции не срабатывать при получении селектором количества событий, указанного в поле **Порог срабатывания селектора (количество событий)**. По умолчанию этот переключатель выключен.
	Пример работы селектора с включенным переключателем Обнуление
	Переключатель **Обнуление** используется в селекторах правил корреляции для сброса контейнера и предотвращения создания корреляционного события. Чаще всего обнуление применяется вместе с действием **По истечении времени жизни контейнера**.
	Правило корреляции типа **standard** настроено следующим образом:
	• В поле **Время жизни контейнера** указано значение `300 секунд`.
	• На вкладке **Действия** настроен триггер **По истечении времени жизни контейнера** с установленным флажком **В дальнейшую обработку**.
	• В правило корреляции добавлено два селектора:
	  • **Virus detected** (в примере событие `{"Message": "virus detected"}`) с выключенным переключателем **Обнуление**.
	  • **Virus deleted** (в примере событие `{"Message": "virus deleted"}`) с включенным переключателем **Обнуление**.
	Когда поступает событие `{"Message": "virus detected"}`, запускается контейнер и происходит следующее:
	• В течение 300 секунд не поступает событие `{"Message": "virus deleted"}`. В этом случае контейнер закрывается и триггер создает корреляционное событие.
	• В течение 300 секунд поступает событие `{"Message": "virus deleted"}`, которое соответствует селектору с включенным переключателем **Обнуление**. В этом случае контейнер очищается и корреляционное событие не создается.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. 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 ↗.
	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`.
	  Вам нужно указать значение 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. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем 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, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

В селекторе корреляционного правила могут быть использованы регулярные выражения, соответствующие стандарту RE2. Применение регулярных выражений в корреляционных правилах создает большую нагрузку в сравнении с другими операциями. При разработке корреляционных правил мы рекомендуем ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Для использования регулярного выражения вам нужно 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, вы можете использовать следующие правила, поставляемые с KUMA:

- R105_04_Подозрительные PowerShell-команды. Подозрение на обфускацию.
- R333_Подозрительное создание файлов в директории автозапуска.

Вкладка Действия

Эта вкладка используется для настройки триггеров правила корреляции. Вы можете настроить триггеры на следующих вкладках:

- **На первом срабатывании правила** – триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.
- **На последующих срабатываниях правила** – триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания селектора.
- **На каждом срабатывании правила** – триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.
- **По истечении времени жизни контейнера** – триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором, в параметрах которого включен переключатель **Обнуление**. Таким образом, триггер срабатывает, если в течение указанного времени жизни ситуация, обнаруженная правилом корреляции, не разрешается.

Доступные параметры триггеров описаны в таблице ниже.

Параметр	Описание

Обогащение	Правила обогащения для изменения значений полей корреляционных событий. Правила обогащения хранятся в правиле корреляции, в котором они были созданы. Для создания правила обогащения нажмите на кнопку **+ Добавить обогащение**. Доступные параметры правила обогащения: • **Исходный тип** – тип обогащения. При выборе определенных типов обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения. Доступные типы обогащения: • **константа** Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения **Параметр** / **Описание** **Константа** – Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено. **Целевое поле** – Поле события KUMA, в которое требуется 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. • **словарь** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения **Параметр** / **Описание** **Название словаря** – Словарь, из которого будут браться значения. **Ключевые поля** – Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий. Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`. • **таблица** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения **Параметр** / **Описание** **Название словаря** – Словарь, из которого будут браться значения. **Ключевые поля** – Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий. **Сопоставление** – Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных. Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря. Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события KUMA, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий KUMA, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.
- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

Обязательный параметр.

- **Отладка** – переключатель, включающий логирование ресурса. По умолчанию этот переключатель выключен.
- **Теги**

Вы можете создать несколько правил обогащения, изменить порядок правил обогащения и удалить правила обогащения. Для изменения порядка правил обогащения используйте значки изменения порядка ⣿. Для удаления правила обогащения нажмите рядом с ним на значок удаления ✕.

В дальнейшую обработку	Флажок, включающий отправку корреляционных событий на *пост-обработку* – на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения. По умолчанию этот флажок снят.
В коррелятор	Флажок, включающий обработку созданного корреляционного события цепочкой правил текущего коррелятора. Это позволят достичь иерархической корреляции. По умолчанию этот флажок снят.

	Если вы устанавливаете флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.
Не создавать алерт	Флажок, выключающий создание алертов при срабатывании правила корреляции. По умолчанию этот флажок снят. Если вы хотите, чтобы алерт не создавался при срабатывании правила корреляции, но корреляционное событие все-равно отправлялось в хранилище, установите флажки **В дальнейшую обработку** и **Не создавать алерт**. Если установлен только флажок **Не создавать алерт**, корреляционное событие не будет сохраняться в хранилище.

Изменение категорий	Правила категоризации для изменения категорий активов, указанных в событии. С помощью правил категоризации вы можете привязывать и отвязывать от активов только реактивные категории. Для создания правила категоризации нажмите на кнопку **+ Добавить категоризацию**.
	Доступные параметры правила категоризации:
	• **Действие** – операция, выполняемая над категорией:
	  • **Добавить** – привязать категорию к активу.
	  • **Удалить** – отвязать категорию от актива.
	  Обязательный параметр.
	• **Поле события** – поле события, содержащее актив, над которым будет выполнена операция.
	  Обязательный параметр.
	• **Идентификатор категории** – категория, над которой будет совершена операция.
	  Обязательный параметр.
	Вы можете создать несколько правил категоризации, изменить порядок правил категоризации и удалить правила категоризации. Для изменения порядка правил категоризации используйте значки изменения порядка ⣿. Для удаления правила категоризации нажмите рядом с ним на значок удаления ✕.

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша ✎.
	  Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **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.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	  Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	  Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе KUMA.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	  Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле KUMA** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка ⣿. Для удаления операции с активным листом нажмите рядом с ней на значок удаления ✕.

Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**.
	Доступные параметры операции с контекстной таблицей:
	• **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша ✎.
	Обязательный параметр.
	• **Операция** – операция, которая выполняется с контекстной таблицей:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `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.
	  • **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.
	  • **Удалить** – удалить запись из контекстной таблицы.
	Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания.
	  • **Поле KUMA** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы.
	  • **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа.
	Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка ⠿. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления ✕.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**, в открывшемся окне укажите один или несколько корреляторов и нажмите на кнопку **OK**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы** → **Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Правило корреляции, тип simple

Правила корреляции с типом **simple** используются для определения простых последовательностей событий. Доступные параметры правила корреляции с типом **simple** описаны в таблицах ниже.

По сравнению с моделью данных нормализованного события некоторые поля корреляционного события, образованного по правилу корреляции **simple**, могут отличаться (см. таблицу ниже).

Название поля корреляционного события	Описание
StartTime	Дата и время создания базового события (timestamp), от которого было образовано корреляционное событие.
EndTime	Дата и время создания базового события (timestamp), от которого было образовано корреляционное событие.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

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.
Тип	Тип правила корреляции – **simple**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Наследуемые поля	Поля событий, по которым отбираются события. Если срабатывает селектор, указанный на вкладке **Селекторы**, отобранные поля событий копируются в корреляционное событие.
Частота срабатываний	Максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: `0`. Если не срабатывают правила корреляции, в которых реализована сложная логика обнаружения закономерностей, причиной могут быть особенности подсчета срабатываний правила в KUMA. В этом случае мы рекомендуем увеличить значение в поле **Частота срабатываний**, например до `1000000`.
Уровень важности	Базовый коэффициент, используемый для определения уровня важности правила корреляции: • **Критический**. • **Высокий**. • **Средний**. • **Низкий** – это значение выбрано по умолчанию.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. 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. • **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 ↗.
	
	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`.
	  Вам нужно указать значение 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. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	
	• Оператор – =.
	
	• Правый операнд – **константа**.
	
	• Значение – значение, по которому требуется фильтровать события.
	
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем 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, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

Вкладка Действия

Эта вкладка используется для настройки триггера правила корреляции. В правиле корреляции с типом **simple** может быть только один триггер, который срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора. Доступные параметры триггера описаны в таблице ниже.

Параметр	Описание

Обогащение	Правила обогащения для изменения значений полей корреляционных событий. Правила обогащения хранятся в правиле корреляции, в котором они были созданы. Для создания правила обогащения нажмите на кнопку **+ Добавить обогащение**. Доступные параметры правила обогащения: • **Исходный тип** – тип обогащения. При выборе определенных типов обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения. Доступные типы обогащения: • **константа** Этот тип обогащения используется, если в поле события необходимо добавить константу. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения | Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения: до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события KUMA, в которое требуется 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. • **словарь** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения | Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий. | Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **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`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['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** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`. • **таблица** Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Доступные параметры типа обогащения описаны в таблице ниже. Доступные параметры типа обогащения | Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных. | Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря. Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `< IP-адрес >|< имя пользователя >`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить элемент**. Для удаления строки таблицы нажмите на кнопку ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события KUMA, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

  Если вы хотите создать правило для изменения исходных данных перед записью в поля событий KUMA, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

  Доступные преобразования

  Преобразования – это изменения, которые применяются к значению перед записью в поле события. Вы можете выбрать в раскрывающемся списке один из следующих типов 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 будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
  - **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 указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
  - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
  - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
    - **Символы на замену** – последовательность символов, которую требуется заменить.
    - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
  - **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
  - **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
  - **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
  - **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
    - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
    - **Чем заменить** – последовательность символов, которую требуется использовать 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, строка будет обрезана и не будет раскодирована.

    Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.
  - Преобразование формата IP-адреса в IPv4:
    - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
    - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками. с октетами, разделенными точками.

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 преобразования.
- для полей с типами `Число` и `Число с плавающей точкой` доступны следующие типы преобразования: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны следующие типы преобразования: **append** и **prepend**.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `", "`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события KUMA, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, 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 следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  Для преобразования в шаблоне данных поля массива в формат TSV необходимо использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

Обязательный параметр.

- **Отладка** – переключатель, включающий логирование ресурса. По умолчанию этот переключатель выключен.
- **Теги**

Вы можете создать несколько правил обогащения, изменить порядок правил обогащения и удалить правила обогащения. Для изменения порядка правил обогащения используйте значки изменения порядка ⠿. Для удаления правила обогащения нажмите рядом с ним на значок удаления ✕.

В дальнейшую обработку	Флажок, включающий отправку корреляционных событий на *пост-обработку* – на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения. По умолчанию этот флажок снят.
В коррелятор	Флажок, включающий обработку созданного корреляционного события цепочкой правил текущего коррелятора. Это позволят достичь иерархической корреляции. По умолчанию этот флажок снят.

	Если вы устанавливаете флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.
Не создавать алерт	Флажок, выключающий создание алертов при срабатывании правила корреляции. По умолчанию этот флажок снят. Если вы хотите, чтобы алерт не создавался при срабатывании правила корреляции, но корреляционное событие все-равно отправлялось в хранилище, установите флажки **В дальнейшую обработку** и **Не создавать алерт**. Если установлен только флажок **Не создавать алерт**, корреляционное событие не будет сохраняться в хранилище.

Изменение категорий	Правила категоризации для изменения категорий активов, указанных в событии. С помощью правил категоризации вы можете привязывать и отвязывать от активов только реактивные категории. Для создания правила категоризации нажмите на кнопку **+ Добавить категоризацию**.
	Доступные параметры правила категоризации:
	• **Действие** – операция, выполняемая над категорией:
	  • **Добавить** – привязать категорию к активу.
	  • **Удалить** – отвязать категорию от актива.
	  Обязательный параметр.
	• **Поле события** – поле события, содержащее актив, над которым будет выполнена операция.
	  Обязательный параметр.
	• **Идентификатор категории** – категория, над которой будет совершена операция.
	  Обязательный параметр.
	Вы можете создать несколько правил категоризации, изменить порядок правил категоризации и удалить правила категоризации. Для изменения порядка правил категоризации используйте значки изменения порядка ⣿. Для удаления правила категоризации нажмите рядом с ним на значок удаления ✕.

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша ✎.
	  Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **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.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	  Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	  Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе KUMA.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	  Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле KUMA** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка ⣿. Для удаления операции с активным листом нажмите рядом с ней на значок удаления ✕.

Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**.
	Доступные параметры операции с контекстной таблицей:
	• **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша ✎.
	Обязательный параметр.
	• **Операция** – операция, которая выполняется с контекстной таблицей:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `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.
	  • **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.
	  • **Удалить** – удалить запись из контекстной таблицы.
	Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания.
	  • **Поле KUMA** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы.
	  • **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа.
	Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка ⠿. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления ✕.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**, в открывшемся окне укажите один или несколько корреляторов и нажмите на кнопку **OK**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы** → **Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Правило корреляции, тип operational

Правила корреляции с типом **operational** используются для работы с активными листами. Доступные параметры правила корреляции с типом **operational** описаны в таблицах ниже.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

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.
Тип	Тип правила корреляции – **operational**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Частота срабатываний	Максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: `0`. Если не срабатывают правила корреляции, в которых реализована сложная логика обнаружения закономерностей, причиной могут быть особенности подсчета срабатываний правила в KUMA. В этом случае мы рекомендуем увеличить значение в поле **Частота срабатываний**, например до `1000000`.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. 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. • **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 ↗.
	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`.
	  Вам нужно указать значение 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. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем 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, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

Вкладка Действия

Эта вкладка используется для настройки триггера правила корреляции. В правиле корреляции с типом **operational** может быть только один триггер, который срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора. Доступные параметры триггера описаны в таблице ниже.

Параметр	Описание

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша.
	Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **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.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе KUMA.
	Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле KUMA** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка. Для удаления операции с активным листом нажмите рядом с ней на значок удаления.

Параметр	Описание

Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**.
	Доступные параметры операции с контекстной таблицей:
	• **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша.
	Обязательный параметр.
	• **Операция** – операция, которая выполняется с контекстной таблицей:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `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.
	  • **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.
	  • **Удалить** – удалить запись из контекстной таблицы.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания.
	  • **Поле KUMA** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы.
	  • **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**, в открывшемся окне укажите один или несколько корреляторов и нажмите на кнопку **OK**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы** → **Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Правило корреляции, тип periodical

Правила корреляции с типом **periodical** используются для выявления несанкционированного использования учетных записей путем обнаружения аномальной активности пользователей, которая может указывать на компрометацию учетной записи. Создание этого правила доступно только при использовании коррелятора correlator-ng.

Механизм анализа событий аутентификации пользователей формирует профиль их обычного поведения и выявляет отклонения от этого поведения на основе статистических показателей. Процесс выявления аномалий выполняется с определенной периодичностью на основе накопленных данных, а не в момент поступления каждого события.

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 выполняется вход.
   - Данные агрегируются по пользователям: сохраняются уникальные значения, формируются значения количества новых адресов для каждого периода группировки событий аутентификации.

   Длительность периода холодного старта является фиксированной и задается в конфигурации правила корреляции. Холодный старт может быть выполнен следующими способами:

   - При обработке потока событий, поступающих в коррелятор.
   - С использованием процедуры ретроспективного сканирования для загрузки событий из хранилища.
   - Комбинированным способом, при котором часть данных загружается с помощью ретроспективного сканирования, а оставшиеся данные накапливаются при обработке потока событий.

   При использовании ретроспективного сканирования правило корреляции обрабатывает загружаемые события так же, как и события, поступающие из потока. Если в хранилище присутствуют события аутентификации пользователей за минимальный период, необходимый для накопления статистики, правило начинает выполнение периодического выявления аномалий сразу после завершения загрузки этих событий.

   Как запустить процедуру ретроспективного сканирования

   Вы можете запустить процедуру ретроспективного сканирования только из консоли, сделать это через веб-интерфейс KUMA невозможно.

   Чтобы выполнить ретроспективное сканирование:

   1. Сформируйте запрос для выгрузки событий.

      Необходимо подготовить запрос к хранилищу событий аутентификации пользователей. Данные должны быть отсортированы по времени создания событий в порядке возрастания.

Пример запроса:

```
SELECT *
FROM `events`
WHERE SourceUserID == 's-1-5-21-1445412355-99643495-187345912-1119' AND Type =
1
ORDER BY Timestamp ASC
LIMIT 250
```

Для правильного отображения идентификаторов событий в журналах коррелятора рекомендуется включить поле идентификатора события при экспорте данных.

2. Экспортируйте результата запроса в файл формата TSV.

   Порядок событий в файле должен соответствовать сортировке по времени создания.

3. Запустите процедуру ретроспективного сканирования из консоли, выполнив следующую команду:

```
/opt/kaspersky/kuma/kuma tools retroscan \
  --url <URL-адрес Ядра KUMA>:<номер порта Ядра KUMA> \
  --src <путь к экспортированному TSV-файлу с событиями> \
  --cert <путь к сертификату Ядра KUMA> \
  --key <путь к ключу для подключения к Ядру KUMA> \
  --alerts
```

   Параметр `--alerts` нужно указать, если нужно создать алерт.

Загруженные события обрабатываются правилом корреляции так же, как и события, поступающие из потока. Если загруженные данные покрывают минимальный период холодного старта, периодическое выявление аномалий начинается сразу после завершения загрузки.

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. **Выявление 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 период выявления аномалий совпадает с периодом группировки, для анализа используется значение показателя за последний завершенный период. Если период выявления меньше периода группировки, анализ выполняется по данным текущего (еще незавершенного) периода, что позволяет получить результаты до окончания всего периода группировки.

   - Вычисляются статистические показатели.

   - Результаты сравниваются с пороговыми значениями, заданными в конфигурации 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)

Где:

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**

  Где:

  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 фиксируется, 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 показателей позволяет оценивать аномалии в разных сценариях поведения, снижая 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.

Создание правила корреляции в коррелятоpe correlator-ng

Вы можете создать правило корреляции типа **periodical** только с помощью коррелятора correlator-ng.

При работе с этим коррелятором следует учитывать, что он использует строгую типизацию данных, поддерживает регулярные выражения по стандарту PCRE и автоматически конвертирует существующие правила в новый формат при первом запуске. Ошибки типизации или некорректные выражения могут привести к тому, что правило не запустится.

Подробнее о работе с коррелятором correlator-ng см. раздел Создание коррелятора correlator-ng

*Чтобы создать правило корреляции с типом **periodical**:*

1. Создайте сервис коррелятора в веб-интерфейсе KUMA.

2. Запустите correlator-ng:
   ```
   /opt/kaspersky/kuma/kuma ng correlator --core <URL_Ядра_KUMA> --id
   <идентификатор_сервиса_коррелятора> --api.port <API-порт_коррелятора> --wd
   <рабочая_директория_коррелятора>
   ```

   Чтобы просмотреть список доступных параметров нужно выполнить следующую команду:

   ```
   /opt/kaspersky/kuma/kuma ng correlator --help
   ```

   При первом запуске коррелятора в рабочей директории будут автоматически созданы конфигурационные файлы, включая директорию config.

3. Остановите коррелятор.

4. Перейдите в директорию config и в файле correlation-rules.yaml укажите параметры правила корреляции, которое нужно создать.

   Описание доступных параметров

   Пример конфигурации правила корреляции типа periodical

```yaml
- id: 69df6a1b-262b-48f0-aab4-be15e822fc86
  name: Lateral movement detection test
  kind: periodical
  selectors:
  - tag: rule fired
    filter: null
    sql: |-
      (
        DeviceEventClassID = '77777'
        AND DeviceProduct = 'Windows'
      )
    recovery: false
    threshold: 0
  identicalFields:
  - SourceUserName
  window: 0
  keepPolicy: all
  orderField: Timestamp
  actions:
    onEveryThreshold:
      output: true
      loop: false
      noAlert: true
      activeLists: null
      contextTables: null
  priority: 1
  lateralMovementDetection:
    thresholds:
      sourceAddress:
        zScore: 12
        relativeScore: 8.5
      destinationAddress:
        zScore: 25
        relativeScore: 45
    minSamples: 15
    detectionPeriod: 60
    eventGroupingPeriod: 1
    propertyValuesCollectingPeriod: 30
    countersCollectingPeriod: 30
    retentionPeriod: 60
    propertyFieldsMapping:
    - sourceEventField: DeviceCustomString1
      destinationProperty: sourceAddress
    - sourceEventField: DeviceCustomString2
      destinationProperty: destinationAddress
```

5. Сохраните изменения в файле.

6. Запустите correlator-ng повторно:

   `/opt/kaspersky/kuma/kuma ng correlator --core <URL_Ядра_KUMA> --id <идентификатор_сервиса_коррелятора> --api.port <API-порт_коррелятора> --wd <рабочая_директория_коррелятора>`

Параметры файла correlation-rules.yaml

В таблице представлены параметры, доступные для настройки правила корреляции типа **periodical** в файле correlation-rules.yaml.

Параметр	Описание
`identicalFields`	Параметр задает одно или несколько полей схемы событий KUMA (уникальные идентификаторы пользователя), по значениям которых события объединяются для анализа активности одного пользователя. Пример значения: `SourceUserName`.
`zScore`	Пороговое значение стандартизованного отклонения (Z-Score). Параметр определяет, насколько текущее значение активности пользователя отклоняется от среднего значения активности с учетом разброса данных. Значение параметра настраивается отдельно для каждого признака детектирования: • Для признака детектирования `sourceAddress`: минимальное значение – `3`, рекомендуемое значение – `12`. • Для признака детектирования `destinationAddress`: минимальное значение – `3`, рекомендуемое значение – `25`.
`relativeScore`	Пороговое значение относительного показателя (Relative Score). Параметр определяет, во сколько раз текущая активность пользователя превышает средний уровень активности за определенный период. Значение параметра настраивается отдельно для каждого признака детектирования: • Для признака детектирования `sourceAddress`: минимальное – `3`, рекомендуемое значение – `8.5`. • Для признака детектирования `destinationAddress`: минимальное значение – `3`, рекомендуемое значение – `45`.
`minSamples`	Минимальное количество событий аутентификации пользователя, необходимых для анализа аномальной активности. Параметр определяет количество событий аутентификации, которое должно быть накоплено, чтобы правило корреляции могло выполнить анализ аномальной активности. Максимальное значение параметра зависит от значений `eventGroupingPeriod` и `countersCollectingPeriod` и определяется количеством периодов группировки данных, доступных для анализа. Максимальное значение можно рассчитать по формуле: `minSamples ≤ countersCollectingPeriod / eventGroupingPeriod`. Минимальное значение – `15`, рекомендуемое значение – `15`. Максимальное значение – `60`.
`detectionPeriod`	Период детектирования. Параметр определяет интервал времени в минутах, через который правило выполняет анализ накопленных событий аутентификации пользователя для выявления аномальной активности. Максимальное значение параметра зависит от значения параметра `eventGroupingPeriod` и рассчитывается по формуле: `detectionPeriod ≤ eventGroupingPeriod * 1440`. Минимальное значение – `15`, рекомендуемое значение – `60`. Максимальное значение – `10080`, при условии, что в параметре `eventGroupingPeriod` указано максимальное значение.
`eventGroupingPeriod`	Период группировки событий. Параметр определяет интервал в днях, за который события аутентификации пользователя объединяются для последующего анализа аномальной активности. Значение параметра влияет на максимально допустимое значение `detectionPeriod`. Анализ выполняется по сгруппированным данным. Минимальное значение – `1`, максимальное значение – `7`, рекомендуемое значение – `1`.
`propertyValuesCollectingPeriod`	Период сбора исторических значений. Параметр определяет интервал в днях, в течение которого уникальные значения анализируемых признаков пользователя накапливаются для последующего анализа аномальной активности. Минимальное значение – `15`, максимальное значение – `60`, рекомендуемое значение – `30`.
`countersCollectingPeriod`	Период сбора счетчиков. Параметр определяет интервал в днях, за который накапливаются данные для формирования показателей аномальной активности. Рассчитать максимальное значение можно по следующей формуле: `countersCollectingPeriod =` число периодов * значение параметра `eventGroupingPeriod`. Рассчитать минимальное значение можно по формуле: `15 *` значение параметра `eventGroupingPeriod`. Минимальное значение – `15`, максимальное значение – `420`, рекомендуемое значение – `30`.

Параметр	Описание
`retentionPeriod`	Период хранения данных правила корреляции. Параметр определяет интервал в днях, в течение которого данные, накопленные правилом, сохраняются для последующего анализа. Рассчитать максимальное значение можно по следующей формуле: `retentionPeriod` = число периодов * значение параметра `eventGroupingPeriod`. Рассчитать минимальное значение можно по формуле: `15` * значение параметра `eventGroupingPeriod`. Минимальное значение – `30`, максимальное значение – `420`, рекомендуемое значение – `60`.
`propertyFieldsMapping`	Маппинги полей для значений анализируемых признаков. Параметр определяет соответствие между полем события KUMA и типом анализируемого признака для выявления аномальной активности пользователей.
`sourceEventField`	Поля события KUMA из схемы событий. Пример значения: `DeviceCustomString1`, `DeviceCustomString2`.
`destinationProperty`	Анализируемые признаки. Возможные значения: `sourceAddress`, `destinationAddress`.

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 $.

Поля расширенной схемы событий могут использоваться в корреляционных правилах, локальных и глобальных переменных.

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 хоста 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 **Сохранить**.

Вы можете ознакомиться с примером использования локальных переменных в правиле, поставляемом с KUMA: R403_Обращение на вредоносные ресурсы с хоста 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 мы рекомендуем 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 **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. Исключением являются простейшие математические операции (сложение, вычитание, умножение, деление), при их использовании скобками обозначается приоритет выполнения операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Должно содержать от 1 до 128 символов в кодировке Unicode.
- 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 тенанта Shared. 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 тенанта Shared. 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 тенанта Shared. 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 из контекстной таблицы.

Необходимо указать параметры в следующей последовательности:

1. Название контекстной таблицы. Название не должно быть пустым.
2. Название поля, значение которого нужно получить.
3. Название ключевого поля, по которому выполняется сравнение.
4. Выражение, возвращающее значение для сравнения со значением ключевого поля из пункта 3.

Функция должна содержать минимум 4 параметра.

Пример использования	Результат выполнения
`context_table('test_table', 'Username', 'IP', DestinationAddress)`	Получение значения указанного поля из строки контекстной таблицы, для которой ключевое поле совпало со значением, переданным в параметре сравнения. Если совпадений нет, отсутствует таблица или поле не найдено, возвращается пустая строка.

С помощью этой функции из переменной можно обратиться к контекстной таблице тенанта Shared. Для этого после названия контекстной таблицы необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `context_table('test_table@Shared', SourceAddress)`.

Функция len

Возвращает длину строки и массива.

Функция возвращает длину массива, если переданный массив соответствует одному из следующих типов:

- 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 одному из следующих типов:

- 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. направление сортировки. Возможные значения: `asc`, `desc`. Если параметр не указан, значение по умолчанию – `asc`.

Функция возвращает отсортированный список элементов массива, если переданный массив соответствует одному из следующих типов:

- 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 `строка`.

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 `строка`. 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 `строка`.

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 `строка`.

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 `строка`.

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 из тех, что доступны 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 строчку `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 строчку `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 из тех, что доступны 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 строчку `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 `строка`.

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

Замена в строке всех вхождений последовательности символов A на последовательность символов B. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

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 `строка`.

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 `строка`.

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. Функция template может быть использована в одном из двух вариантов:

- Когда у функции только один аргумент. В этом случае можно использовать имена полей для подстановки значений в шаблон.
- Когда у функции несколько аргументов. В этом случае для подстановки значений используется индекс аргумента, начинающийся с нуля.

Примеры использования
• `template('Текст сообщения: {{.Message}}')` • `template('Имя в нижнем регистре: {{index . 0}}. Имя в верхнем регистре: {{index . 1}}', to_lower(Name), to_upper(Name))`

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. (необязательно) Обозначение часового пояса. 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')`

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. Поддерживается 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. Поддерживается 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. Поддерживается 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. Поддерживается 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. Поддерживается 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 или вещественные 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. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Параметры необходимо указать в следующей последовательности:

1. Разделитель. Строка.
2. Строка 1, строка 2, строка N. 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. Поддерживается 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 веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** выберите набор ресурсов нужного коррелятора.

   Откроется мастер установки коррелятора.

2. Выберите шаг мастера установки **Глобальные переменные**.
3. 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.
     - Должно содержать от 1 до 128 символов в кодировке Unicode.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

     Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

Описание функций переменных.

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

4. 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 веб-интерфейсе KUMA в разделе **Ресурсы** → **Правила корреляции** выберите нужное 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**.

2. Откройте вкладку **Селекторы**.

3. 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.
     - Должно содержать от 1 до 128 символов в кодировке Unicode.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

     Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

     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.

4. Нажмите **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.

Добавление временного списка исключений для корреляционного правила

Для пользователей без прав редактирования корреляционных правил в веб-интерфейсе KUMA имеется возможность создавать временный список исключений (например, создавать исключения для ложноположительных срабатываний при работе с 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. Нажать 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.
- `Корреляционное правило`

  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.

- `Истекает`

Дата и время, когда исключение будет автоматически удалено из списка.

- `Создано`

  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** → **Другое** → **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**.

Предустановленные правила корреляции

В поставку KUMA 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 of time	Выявляет факты создания и последующего удаления учетных записей на хостах на базе ОС Microsoft Windows.
[OOTB][AD] An account failed to log on from different hosts	Выявляет множественные неуспешные попытки аутентификации на различных хостах.
[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 хосте от имени разных учетных записей.
[OOTB][AD] Successful authentication with the same account on multiple hosts	Выявляет подключения на разные хосты 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 of time	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.

Техники и тактики MITRE ATT&CK

Все операции с техниками и тактиками MITRE ATT&CK доступны только после импорта списка техник MITRE ATT&CK.

В KUMA доступны следующие возможности:

- Обогащение корреляционных событий информацией о техниках и тактиках MITRE ATT&CK.

  Для этого используются поля модели данных события Tactic и Technique. При генерации корреляционного события можно заполнять эти поля соответствующими данными для последующего использования. Например, при получении нового алерта с разметкой по MITRE ATT&CK, вы можете открыть сайт MITRE ATT&CK и ознакомиться с описанием техник и тактик, когда, каким образом и для чего злоумышленники могут использовать эти техники, как их обнаруживать и митигировать риски - все это поможет разработать план реагирования. Также вы можете строить отчеты и панели мониторинга, исходя из того, какие алерты и техники были замечены в инфраструктуре. Если вы используете правила корреляции из пакета SOC_package и хотите настроить обогащение корреляционных событий информацией о техниках и тактиках MITRE ATT&CK, добавьте в корреляторе правила обогащения MITRE.

- Оценка покрытия матрицы MITRE ATT&CK вашими корреляционными правилами.

  В этом случае используются общие настройки корреляционного правила, где есть возможность привязать к каждому правилу соответствующие техники MITRE. Этот параметр используется для описания самого правила и эти данные никак не передаются в корреляционное правило или алерт. Привязка техник и тактик к правилам корреляции позволяет проанализировать покрытие матрицы MITRE ATT&CK, фокусируясь на техниках, наиболее релевантных для конкретной инфраструктуры.

  Если вы хотите оценить покрытие матрицы MITRE ATT&CK вашими корреляционными правилами, выполните следующие шаги:

  1. Скачайте справочник техник из официального репозитория MITRE ATT&CK и импортируйте справочник техник в KUMA.
  2. Привяжите техники MITRE ATT&CK к правилам корреляции.
  3. Экспортируйте правила корреляции в MITRE ATT&CK Navigator.

  В результате вы сможете визуально оценить покрытие матрицы MITRE ATT&CK.

- Визуализация покрытия матрицы MITRE ATT&CK продуктами "Лаборатории Касперского".

Добавление в корреляторе правил обогащения MITRE

Чтобы добавить правила обогащения MITRE из пакета SOC_package:

1. В разделе KUMA **Ресурсы и сервисы** → **Корреляторы** нажмите **Добавить**, чтобы создать коррелятор, или выберите действующий коррелятор в списке, чтобы перейти в режим редактирования параметров.

2. В мастере установки коррелятора на шаге **Обогащение** нажмите **Добавить обогащение**.

3. В открывшемся окне **Обогащение** в раскрывающемся списке **Правило обогащения** выберите правила **MITRE Technique** и **MITRE Tactics**.

   Правила обогащения **MITRE Technique** и **MITRE Tactics** преднастроены, никаких дополнительных параметров указывать не требуется.

4. Сохраните параметры коррелятора.

5. Если вы создали коррелятор, необходимо выполнить установку сервиса коррелятора на хосте. Если вы редактировали параметры действующего коррелятора, сервис коррелятора необходимо перезапустить.

Правила обогащения **MITRE Technique** и **MITRE Tactics** добавлены.

Импорт списка техник MITRE ATT&CK

Импорт списка техник MITRE ATT&CK доступен только пользователю с ролью Главный администратор.

Чтобы импортировать список техник MITRE ATT&CK:

1. Скачайте справочник техник MITRE ATT&CK на портале GitHub.

   KUMA версии 4.2 поддерживает работу только со справочником техник MITRE ATT&CK начиная с версии 14.2, рекомендуемая версии справочника для использования 19.2.

2. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие**.

3. В разделе **Настройки списка техник MITRE** нажмите на кнопку **Импортировать из файла**.

   Откроется окно выбора файлов.

4. Выберите скачанный справочник техник MITRE ATT&CK и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Список техник MITRE ATT&CK будет импортирован в KUMA. Вы можете увидеть список импортированных техник и версию справочника техник MITRE ATT&CK, нажав на кнопку **Просмотреть список**.

Привязка техник MITRE ATT&CK к правилам корреляции

Чтобы привязать техники MITRE ATT&CK к правилам корреляции:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Правила корреляции**.
2. Откройте окно редактирования правила корреляции, нажав на имя правила корреляции.

   Откроется окно редактирования правила корреляции.
3. Во вкладке **Общие** при нажатии на поле **Техники MITRE** откроется список доступных техник. Для удобства поиска доступен фильтр: в поле можно ввести название техники, ID техники или тактики. Для привязки к правилу корреляции доступна одна или несколько техник MITRE ATT&CK.
4. Нажмите на кнопку **Сохранить**.

Техники MITRE ATT&CK будут привязаны к правилу корреляции. В веб-интерфейсе в разделе **Ресурсы** → **Правила корреляции** в столбце **Техники MITRE** у отредактированного правила отобразится ID выбранной техники, а при наведении курсора на элемент отобразится полное название техники с указанием ID техники и тактики.

Экспорт правил корреляции в MITRE ATT&CK Navigator

Чтобы экспортировать правила корреляции с привязанными техниками в MITRE ATT&CK Navigator:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Правила корреляции**.
2. В правом верхнем углу нажмите на кнопку **...**.
3. В раскрывающемся списке нажмите на кнопку **Экспортировать в MITRE ATT&CK Navigator**.
4. В открывшемся окне выберите правила корреляции, которые вы хотите экспортировать.
5. Нажмите на кнопку **OK**.

   Файл с экспортированными правилами будет загружен на ваш компьютер.
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.

Конвертер правил Sigma

Конвертер правил Sigma преобразует правила корреляции в понятный KUMA формат и упрощает импорт простых правил для последующей доработки аналитиком.

Работа конвертера правил Sigma поддерживается на следующих операционных системах:

- Ubuntu 2024.
- Windows 10, 11.

- РЕДОС 7, 8.
- OracleLinux 8.3, 9.3.

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 установить конвертер:

     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` и другим портом, например `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 будет установлен.

- **Установка конвертера правил Sigma в среде, допускающей запуск образов docker**

  Этот метод установки использует предоставленный контейнер и позволяет создать сервис systemd и развернуть веб-интерфейс с помощью Kubernetes.

  Подойдет любой инструмент запуска контейнеров, например docker, podman или 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:

     - С помощью команды:

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
       ```

       Дождитесь, когда команда будет выполнена или перейдет в состояние ожидания. Не нажимайте **Ctrl**+**C**, пока процесс установки не будет завершен или пока не будет явно предложено прервать установку

     - Запуск в фоновом режиме:

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
       ```

  Конвертер будет установлен.

- **Установка конвертера правил Sigma с использованием Python 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 установить конвертер:

  1. Убедитесь, что установлен Python 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 хост, 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 укажите переменные окружения `HOST` и `PORT`, чтобы настроить слушающий интерфейс и задать номер порта.

Конвертер будет 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.

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 KUMA.
- `src/sigconverter.io/README.md` – пользовательский веб-интерфейс.

После установки войдите в веб-интерфейс конвертера.

2. Доработайте правило корреляции в конвертере правил Sigma и скопируйте или импортируйте доработанное правило в KUMA.

3. Перезапустите коррелятор, чтобы применить изменения.

Доработанное вами правило корреляции применяется в корреляторе.

Подготовка правила Sigma

Чтобы конвертировать правило Sigma в правило KUMA:

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, мы рекомендуем в исходном правиле Sigma приводить соответствующие поля к нижнему регистру.

   - Мы не рекомендуем в условиях `contains` и подобных условиях писать комментарии или дополнительную информацию. В случае необходимости оставить комментарий мы рекомендуем 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 KUMA 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 /api/v2.1/resources/correlationRule/create с указанием tenantID и имени тенанта для импорта.

4. Перейдите на вкладку конвертера **custom_pipeline.yml** и скопируйте на эту вкладку "**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 KUMA, если это запрос или фильтр. Если вы хотите использовать в KUMA правило, можно импортировать в KUMA по одному правилу.

Поддерживаемые примеры конвертации правил Sigma

Поддерживаемые примеры конвертации правил Sigma

Правило Sigma	Сопоставление с объектами KUMA	
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 передать в Unique fields, все, что после 'by' Computer → DestinationHostName LogonID → FlexString1 передать в Aggregation fields, все, что после '=' или '>' 2 передать в threshold. timeframe передать в time window	Для корреляцион реализована част условия condition условие селектор запрос для Поиск

Правило Sigma	Сопоставление с объектами KUMA	
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: в условии `condition` используется конструкция `1 of selection`, где `selection` обозначает одну из именованных групп условий.	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 KUMA	
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 KUMA	
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 KUMA	
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	

Фильтры

Фильтры позволяют отбирать события на основании указанных условий. В сервисе коллектора фильтры используются для отображения событий, которые вы хотите передавать в KUMA. События, удовлетворяющие условия фильтра, будут переданы в KUMA для дальнейшей обработки.

Вы можете использовать фильтры в следующих сервисах и функциях KUMA:

- Коллектор.
- Коррелятор.
- Хранилище.
- Правила корреляции.
- Правила обогащения.
- Правила агрегации.
- Точки назначения.
- Правила реагирования.
- Правила сегментации.

Вы можете использовать отдельные фильтры или встроенные фильтры, которые хранятся в сервисе или ресурсе, в котором они были созданы. Для ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов. Доступные параметры фильтра описаны в таблице ниже.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр. Встроенные фильтры создаются в других ресурсах или сервисах и не имеют имен.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вы можете создавать условия фильтрации и группы фильтров, а также добавлять в фильтр существующие фильтры.

Для формирования критериев фильтрации вы можете использовать *режим конструктора* или *режим исходного кода*. 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. По умолчанию используется режим конструктора.

Вы можете переключаться между режимами при формировании критериев фильтрации. Для переключения в режим исходного кода выберите вкладку **Код**. При переключении между режимами сформированные фильтры условий сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

Формирование критериев фильтрации в режиме конструктора

Для формирования критериев фильтрации в режиме конструктора вам нужно выбрать один из следующих операторов в раскрывающемся списке:

- **И** – фильтр отбирает события, которые соответствуют всем указанным условиям.
- **ИЛИ** – фильтр отбирает события, которые соответствуют одному из указанных условий.
- **НЕ** – фильтр отбирает события, которые не соответствуют всем указанным условиям.

Критерии фильтрации можно добавить одним из следующих способов:

- Если вы хотите добавить условие, нажмите на кнопку **+ Добавить условие**.
- Если вы хотите добавить группу условий, нажмите на кнопку **+ Добавить группу**. При добавлении групп условий вы также можете выбирать операторы **И**, **ИЛИ** и **НЕ**. В группу условий в свою очередь можно добавить условия и группы условий.

Вы можете добавить несколько критериев фильтрации, изменить порядок критериев фильтрации и удалить критерии фильтрации. Для изменения порядка критериев фильтрации используйте значки изменения порядка ⣿. Для удаления критерия фильтрации нажмите рядом с ним на значок удаления ✕.

Доступные параметры условия описаны в таблице ниже.

Параметр	Описание
<Тип условия>	Тип условия. По умолчанию выбрано значение **Если**. Вы можете нажать значение по умолчанию и выбрать в отобразившемся раскрывающемся списке значение **Если не**. Обязательный параметр.

<Левый операнд> и **<Правый операнд>**	Значения, которые будет обрабатывать оператор. Доступные типы значений для правого операнда зависят от выбранного оператора.
	Операнды фильтров
	• **Поля событий** – в этом разделе вы можете указать поле событие, которое требуется использовать как операнд фильтра.
	• **Активные листы** – в этом разделе вы можете указать активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа вам нужно указать одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш `Ctrl`/`Command`+`F1`.
	Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
	• **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
	  • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
	  • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
	  • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
	  • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
	• **Словарь** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
	  • **словарь** (обязательно) – словарь, который требуется использовать.
	  • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Таблица** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
	  • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	• **TI** – параметры чтения данных CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз CyberTrace.
	  • **поле** (обязательно) – поле фида CyberTrace с индикаторами угроз.
	Обязательные параметры.

Параметр	Описание
<Оператор>	Оператор условия. При выборе оператора условия в раскрывающемся списке вы можете установить флажок **без учета регистра**, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **inSubnet**, **inActiveList**, **inCategory**, **InActiveDirectoryGroup, hasBit** и **inDictionary**. По умолчанию этот 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. Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него, после чего нажмите на клавишу **`Backspace`**.

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	—	—	—	—	—	—	—	—

При работе с фильтрами вы можете использовать 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` вы можете использовать следующие операции:

- Операция `contains` вернет значение `True`, если указанная подстрока присутствует в массиве, иначе вернет `False`.
- Операция `match` – поиск в строке по регулярному выражению.
- Операция `intersec`.

Формирование критериев фильтрации в режиме исходного кода

Режим исходного кода позволяет быстро изменять условия, выделять и копировать блоки кода. В правой части конструктора отображается навигатор для перемещения по 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, невозможно изменить. Названия категорий общих ресурсов не отображаются в фильтре, если вам не назначена роль Чтение общих ресурсов. Для просмотра списка ресурсов для выбранного операнда внутри выражения вам нужно нажать на комбинацию клавиш **`Ctrl+Space`**. В результате отобразится список ресурсов.

В поставку KUMA 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 безуспешной 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 использованием пароля по протоколу SSH.
[OOTB][SSH] Failed Password	Выбирает события попыток подключения с использованием 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 правило корреляции типа operational и добавить в активный лист эти IP-адреса.

2. Создать правило корреляции 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 правил корреляции типа simple или импортировать файл с данными для активного листа.

Вы можете добавлять, копировать и удалять активные листы.

Активные листы можно использовать в правилах корреляции и панелях 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. Активный лист следует привязать к правилу корреляции, а правило корреляции привязать к коррелятору.

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.

> Если во время работы с данными активного листа коррелятор выключен, то в интерфейсе отображается ошибка "Internal communication failed", сообщающая о том, что потеряно соединение с источником данных, а именно потеряно соединение с коррелятором.

В процессе корреляции при удалении записей из активных листов по истечении срока жизни записи 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 обрабатывать эти события и 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
`Name`	`active list record expired`
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`ServiceID`	Идентификатор коррелятора
`ServiceName`	Название коррелятора
`DeviceExternalID`	Идентификатор активного листа
`DevicePayloadID`	Ключ записи, срок жизни которого истек
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи
S.<поле активного листа>	Выпавшая запись активного листа в формате: S.<поле активного листа> = <значение активного листа>

Просмотр таблицы активных листов коррелятора

Чтобы просмотреть таблицу активных листов коррелятора:

1. В веб-интерфейсе KUMA выберите **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.
2. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

Описание таблицы Активные листы коррелятора

Название столбца	Описание
Название	Название активного листа.
Записи	Количество записей в активном листе.
Размер на диске	Место, которое активный лист занимает на диске, КБ.
Каталог	Путь к активному листу на сервере коррелятора KUMA.

Добавление активного листа

Чтобы добавить активный лист:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами.
2. В веб-интерфейсе KUMA выберите раздел **Ресурсы** → **Ресурсы** → **Активные листы**.
3. На панели инструментов или в меню (⋮) нажмите **Добавить активный лист**.
4. Выполните следующие действия:

   a. В поле **Название** введите название активного листа.

   b. В раскрывающемся списке **Тенант** укажите тенант, которому принадлежит ресурс.

   c. В поле **Срок жизни** укажите время в секундах, 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 36 000 дней (около 100 лет).

   d. При необходимости в поле **Теги** укажите теги для поиска ресурса.

   e. При необходимости в поле **Описание** введите дополнительную информацию.

      Вы можете использовать до 4000 символов в кодировке Unicode.

5. Чтобы сохранить активный лист, выберите один из следующих вариантов:

   - Нажмите на кнопку **Сохранить**.

   - Нажмите на кнопку **Сохранить с комментарием**.

     При необходимости в появившемся окне **Оставить комментарий** добавьте комментарий. Чтобы просмотреть комментарии для активного листа, в таблице активных листов установите флажок рядом с нужным активным листом и на панели инструментов или в меню (⋮) нажмите **Показать историю версий**. В появившемся окне **История версий** будет отображаться таблица со списком доступных версий активного листа и вы сможете просмотреть комментарии.

Активный лист будет добавлен.

Просмотр параметров активного листа

Чтобы просмотреть параметры активного листа:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами.

2. В веб-интерфейсе KUMA выберите **Ресурсы** → **Ресурсы** → **Активные листы**.

   Отобразится таблица доступных активных листов.

3. В столбце **Название** выберите активный лист, параметры которого вы хотите просмотреть.

Отобразятся параметры активного листа. См. описание параметров активного листа в следующей таблице.

Описание параметров активного листа

Название параметра	Описание
ID	Идентификатор активного листа.
Название	Уникальное название активного листа.
Тенант	Название тенанта, которому принадлежит активный лист.
Срок жизни	Время, в течение которого в активном листе будет храниться добавленная в него запись. Указывается в секундах.
Теги	Теги для поиска активного листа.
Описание	Любая дополнительная информация об активном листе.
Коррелятор	Имя коррелятора, к которому привязан активный лист. Поле отображается, если активный лист привязан к коррелятору.

Если активный лист привязан к коррелятору, отображается таблица значений активного листа.

Изменение параметров активного листа

Чтобы изменить параметры активного листа:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами.
2. В веб-интерфейсе KUMA выберите **Ресурсы** → **Ресурсы** → **Активные листы**.

   Отобразится таблица доступных активных листов.
3. В столбце **Название** выберите активный лист, параметры которого вы хотите изменить.
4. Измените необходимые параметры:
   - **Название** – уникальное название активного листа.
   - **Срок жизни** – время в секундах, в течение которого в активном листе будет храниться добавленная в него запись.

     Если в поле указано значение 0, запись хранится 36 000 дней (около 100 лет).
   - **Теги** – теги для поиска активного листа.
   - **Описание** – любая дополнительная информация об активном листе.

   Параметры **ID**, **Тенант** и **Коррелятор** недоступны для редактирования.

Дублирование активного листа

Чтобы скопировать активный лист:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами.
2. В веб-интерфейсе KUMA выберите **Ресурсы** → **Ресурсы** → **Активные листы**.
3. Установите флажок рядом с активным листом, который вы хотите скопировать.
4. На панели инструментов или в меню (⋮), нажмите **Дублировать**.
5. Укажите название листа и тенант, в который вы хотите скопировать активный лист. По умолчанию активному листу, который вы дублируете, присваивается имя в формате <Название_активного_листа>-копия, а также он дублируется в тот тенант, в котором вы сейчас находитесь.

6. Чтобы сохранить активный лист, выберите один из следующих вариантов:

   - Нажмите на кнопку **Сохранить**.

   - Нажмите на кнопку **Сохранить с комментарием**.

     При необходимости в появившемся окне **Оставить комментарий** добавьте комментарий. Чтобы просмотреть комментарии для активного листа, в таблице активных листов установите флажок рядом с нужным активным листом и на панели инструментов или в меню (⋮) нажмите **Показать историю версий**. В появившемся окне **История версий** будет отображаться таблица со списком доступных версий активного листа и вы сможете просмотреть комментарии.

Активный лист будет скопирован.

Удаление активных листов

Чтобы удалить активные листы:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами.

2. В веб-интерфейсе KUMA выберите **Ресурсы** → **Ресурсы** → **Активные листы**.

3. Установите флажки рядом с активными листами, которые вы хотите удалить.

   Если вы хотите удалить все активные листы, установите флажок рядом со столбцом **Название** и в отобразившемся контекстном меню выберите одну из следующих опций:

   - **Выбрать все**.

   - **Выбрать все на странице**.

   Должен быть установлен хотя бы один флажок.

4. Нажмите на кнопку **Удалить**.

5. В окне подтверждения нажмите **Удалить**.

   Если на выбранные активные листы есть ссылки из других ресурсов и сервисов, удаление будет недоступно. В таком случае необходимо сначала отвязать активные листы от корреляционных правил и корреляторов.

Активные листы будут удалены.

Просмотр записей в активном листе

Чтобы просмотреть список записей в активном листе:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

- Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

  Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

  На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

  Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

Откроется таблица записей для выбранного активного листа. Если активный лист привязан к коррелятору, отображается таблица значений активного листа.

Описание таблицы записей активного листа

Название параметра	Описание
Ключ	Название ключа активного листа. Можно указать несколько значений, используя символ | .
Значение	Значение ключа активного листа. Можно указать несколько значений ключа через запятую в формате JSON.
Действия	Действия, доступные с записями активного листа. Вы можете изменять или удалять 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 будет удалена. Если при создании активного листа в поле **Срок жизни** было указано значение 0, записи этого активного листа хранятся 36 000 дней (около 100 лет).
Последнее обновление	Время последнего обновления активного листа.

На странице отображается не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Поиск записей в активном листе

Чтобы найти запись в активном листе:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей выбранного активного листа.

3. В поле **Поиск** введите название ключа записи или несколько символов из названия. Также вы можете выполнить поиск по значению ключа.

В таблице записей активного листа отобразятся только те записи, в значении которых есть введенные символы.

Добавление записи в активный лист

Чтобы добавить запись в активный лист:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выберите один из следующих вариантов:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Нажмите на кнопку **Добавить**.

4. Укажите значения для следующих параметров:

   a. В поле **Ключ** введите имя записи.

      Вы можете указать несколько значений, используя символ `|`.

   b. В поле **Значение** укажите значение в формате JSON. Вы можете указать несколько значений.

5. Нажмите на кнопку **Сохранить**.

   Запись будет добавлена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Дублирование записей в активном листе

Чтобы дублировать запись в активном листе:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Установите флажок рядом с записью, которую вы хотите скопировать.

4. Нажмите на кнопку **Дублировать**.

5. Укажите ключ и при необходимости измените значения ключа.

6. Нажмите на кнопку **Сохранить**.

   Запись будет скопирована. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Изменение записи в активном листе

Чтобы изменить запись в активном листе:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Нажмите на значок карандаша в столбце **Действия**.

4. Измените требуемые значения ключа в формате JSON.

5. Если вы хотите подтвердить изменения, нажмите на галочку в столбце **Действия**. Если вы хотите отменить изменения, нажмите на значок крестика в столбце **Действия**.

6. Нажмите **Сохранить**.

   Запись будет изменена. После сохранения записи в активном листе будут выстроены в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Удаление записей в активном листе

Чтобы удалить записи из активного листа:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Установите флажки рядом с записями, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   > Должен быть установлен хотя бы один флажок.

4. Нажмите на кнопку **Удалить**.

5. Нажмите на кнопку **Ок**.

Записи будут удалены.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Импорт записей в активный лист

Чтобы импортировать записи в активный лист:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.Нажмите на название активного листа и в открывшемся окне **Редактирование активного листа** в секции **Контент** установите флажки рядом с записями, которые вы хотите импортировать.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

В отобразившейся таблице **Активные листы коррелятора** установите флажок рядом с требуемым активным листом.

2. В панели инструментов нажмите **Импортировать**.

   Откроется окно импорта активного листа.

3. Нажмите на кнопку **Добавить** и в открывшемся окне выберите файл, который требуется импортировать.

4. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**;
   - **tsv**;
   - **internal**.

5. В поле **Ключевое поле** введите название столбца с ключами записей активного листа, который указан в файле. Поле недоступно для формата **internal**.

6. 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 записей из активного листа

Чтобы экспортировать записи активного листа:

1. В веб-интерфейсе KUMA выберите тенанты, в рамках которых вы планируете работать с активными листами, и выполните одно из следующих действий:

   - Перейдите в раздел **Ресурсы** → **Ресурсы** → **Активные листы**.

     Отобразится таблица доступных активных листов.Нажмите на название активного листа и в открывшемся окне **Редактирование активного листа** в секции **Контент** установите флажки рядом с записями, которые вы хотите экспортировать.

   - Перейдите в раздел **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.

     Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     В панели инструментов или в меню ⋮ нажмите **Смотреть активные листы**.

     В отобразившейся таблице **Активные листы коррелятора** установите флажок рядом с требуемым активным листом.

2. В панели инструментов нажмите **Экспортировать**.

Активный лист будет загружен в формате JSON в папку по умолчанию или в папку, указанную в параметрах вашего браузера. Название загруженного файла соответствует названию активного листа.

Предустановленные активные листы

В поставку KUMA включены перечисленные в таблице ниже активные листы.

Предустановленные активные листы

Название 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 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 хостами под управлением ОС Linux. Записи удаляются из списка через 24 часа после внесения.

Прокси-серверы

Прокси-серверы используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http. Доступные параметры прокси-сервера описаны в таблице ниже.

Доступные параметры прокси-сервера

Параметр	Описание
Название	Уникальное имя прокси-сервера. Максимальная длина имени: от 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Секрет отдельно	Просмотр информации о подключении. Если флажок установлен, в окне отображаются следующие параметры: • **URL** – URL подключения. • **Секрет** – секрет типа credentials. Вы сможете просматривать информацию о подключении и вам не придется повторно создавать большое количество подключений при изменении пароля учетной записи, которую вы использовали для подключений. По умолчанию флажок снят.
Брать URL из секрета	Ресурс секрета, в котором хранятся URL прокси-серверов. Вы можете создать и изменить секрет. Для создания секрета нажмите на значок плюса (+). Для изменения секрета нажмите на значок карандаша ( ). Мы не рекомендуем использовать этот параметр. Вместо этого указывайте URL и секрет отдельно вручную, установив флажок **Секрет отдельно**.
Не использовать на доменах	Один или несколько доменов, к которым требуется прямой доступ.
Описание	Описание прокси-сервера. Максимальная длина описания: до 4000 символов в кодировке Unicode.

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 словаря описаны в таблице ниже.

Доступные параметры словаря

Параметр	Описание
Название	Уникальное имя для этого типа ресурса. Максимальная длина имени: до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания: до 4000 символов в кодировке Unicode.
Тип	Тип словаря. От выбранного типа словаря зависит формат данных, которые может содержать словарь: • В тип **Словарь** можно добавлять пары ключ–значение. Мы не рекомендуем добавлять в словари этого типа более 50 000 записей через веб-интерфейс KUMA. 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. Вы можете взаимодействовать с этим типом словарей можно с помощью REST API. При добавлении словарей через API ограничение на количество записей отсутствует. Обязательный параметр.
Значения	Таблица с данными словаря. • Для типа **Словарь** в блоке отображается перечень пар **Ключ** – **Значение**. Вы можете добавлять и удалять строки из таблицы. Для добавления строки в таблицу нажмите на кнопку +. Для удаления строки из таблицы наведите курсор мыши на строку таблицы и нажмите на отобразившуюся кнопку ×. В поле **Ключ** вам нужно указать уникальный ключ. Максимальная длина ключа: 128 символов в кодировке Unicode. Первый символ не может быть $. В поле **Значение** вам нужно указать значение. Максимальная длина значения: 255 символов в кодировке Unicode. Первый символ не может быть $. Вы можете добавить одну или несколько пар **Ключ** – **Значение**. • Для типа **Таблица** в блоке отображается таблица с данными. Вы можете добавлять и удалять строки и столбцы из таблицы. Для добавления строки или столбца в таблицу нажмите на кнопку +. Для удаления строки или столбца из таблицы наведите курсор мыши на строку или заголовок столбца таблицы и нажмите на отобразившуюся кнопку ×. Заголовки столбцов таблицы можно редактировать. Если словарь содержит больше 5000 записей, они не отображаются в веб-интерфейсе 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

Данные словарей можно импортировать или экспортировать 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 в кодировке Unicode.

  Значения должны содержать от нуля до 256 символов в кодировке Unicode.

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 ("). Кроме того, 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

С помощью REST API можно считывать содержимое словарей типа **Таблица**, а также изменять его, 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 KUMA включены перечисленные в таблице ниже словари.

Предустановленные словари

Название словаря	Тип	Описание
[OOTB] Ahnlab. Severity	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 **Priority** 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, KATA, Active Directory и запуск пользовательского скрипта.

Автоматическое выполнение задач Kaspersky Security Center, Kaspersky Endpoint Detection and Response, KICS for Networks, KATA и Active Directory по правилам реагирования доступно при интеграции с перечисленными программами.

Вы можете настроить правила реагирования в разделе **Ресурсы** → **Реагирование**, а затем выбрать созданное правило реагирования в раскрывающемся списке в настройках коррелятора. Правила реагирования также можно настроить напрямую 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

Вкладка Общие

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр, доступен при интеграции KUMA с Kaspersky Security Center. Тип правила реагирования, **ksctasks**.

Параметр	Описание
Задача Kaspersky Security Center	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.
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения: • SourceAssetID. • DestinationAssetID. • DeviceAssetID.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание правила реагирования. Вы можете добавить до 4000 символов в кодировке Unicode.

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** 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 ↗.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если правила реагирования принадлежат тенанту Shared, 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 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 отвязать правило реагирования от сервиса. 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 решение 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

Вкладка Общие

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
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}}"`
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов в кодировке Unicode.

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** 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 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 отвязать правило реагирования от сервиса. 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

Вкладка Общие

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **Реагирование через KICS/KATA**.
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**.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов в кодировке Unicode.

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** 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 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 отвязать правило реагирования от сервиса. 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

Вкладка Общие

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 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 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 программы. 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 программу. 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 решения отобразится задача **Запустить программу**. 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 программы.
	  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.

Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание правила реагирования. Вы можете добавить до 4000 символов в кодировке Unicode.

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** 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 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 отвязать правило реагирования от сервиса. 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

Вкладка Общие

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **Реагирование через Active Directory**.
Источник идентификатора учетной записи	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 необходимо переместить учетную запись. В обязательном для заполнения поле **Distinguished name** 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 необходимо переместить учетную запись. В обязательном для заполнения поле **Distinguished name** 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
DN группы	DistinguishedName группы домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для каждой роли. Пример ввода группы: OU=KUMA users,OU=users,DC=example,DC=domain
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

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** 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.

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 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 отвязать правило реагирования от сервиса. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила реагирования с EDR-действиями

Начиная с версии KUMA 3.4.1 и Kaspersky Endpoint Security для Windows 12.9 добавлена поддержка EDR-действий при реагировании на угрозы. При получении корреляционных событий KUMA будет выполнять EDR-действия. Для выполнения EDR-действий вам нужно предварительно настроить правила реагирования. В свойствах правил реагирования следует задать аргументы скриптов, которые доступны для скачивания по следующей ссылке:

https://box.kaspersky.com/d/579c0271a38e440b9144/

При срабатывании правила реагирования Kaspersky Endpoint Security выполняет EDR-действия и создает в Kaspersky Security Center следующие задачи:

- onDemandScan.py – проверка важных областей.
- ioCScan.py – поиск индикаторов компрометации.
- quarantineFile.py – помещение файла на карантин.
- deleteFile.py – удаление файла.
- getFile.py – получение файла.
- isolateHost.py – сетевая изоляция компьютера.

- preventExecution.py – запрет запуска объектов.

  Для выполнения этой задачи важно убедиться, что в Kaspersky Security Center в разделе **Активы (Устройства)** → **Политики и профили политик** → <название политики Kaspersky Endpoint Security> → **Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response** переключатель **Запрет запуска ВЫКЛЮЧЕН** находится в неактивном положении.

- startProcess.py – запуск процесса.

- terminateProcess.py – завершение процесса.

При настройке правил реагирования с EDR-действиями мы рекомендуем учитывать нагрузку на компьютер при запуске задач. Если в результате работы правил реагирования скрипты создадут слишком много задач, производительность компьютера может снизиться. Если запросов будет слишком много, будет выполняться ротация запросов независимо от того, был ли выполнен запрос. Kaspersky Endpoint Security позволяет создавать не более 100 задач. При достижении этого ограничения Kaspersky Endpoint Security выполняет ротацию задач в Kaspersky Security Center. Срок жизни задачи составляет 30 дней.

> Задачи, создаваемые при выполнении правил реагирования из KUMA, отображаются в Kaspersky Endpoint Security того хоста, на котором запущено правило реагирования. В Kaspersky Security Center эти задачи не отображаются.

Информацию о выполнении EDR-действий вы можете посмотреть в Консоли администрирования Kaspersky Security Center с помощью отчетов. Kaspersky Endpoint Security формирует события с описанием в формате '[Response][kuma] $<script name> - $<date>';. Описание в таком формате позволяет создавать выборки событий для EDR-действий.

Настройка правил реагирования с EDR-действиями

Предварительные условия

Перед настройкой правил реагирования с EDR-действиями убедитесь, что выполнены следующие условия:

1. Настроена интеграция с Kaspersky Security Center.

2. В Kaspersky Security Center создан отдельный пользователь, у которого есть права на выполнение всех задач Kaspersky Endpoint Security и задач, которые вы планируете запускать с помощью скриптов.

3. Настроена интеграция с Kaspersky Endpoint Security для Windows. При установке Kaspersky Endpoint Security необходимо установить компонент EDR.

4. На хосте с коррелятором выполнены следующие действия:

   a. Установлен Python версии 3.6 или выше и пакет Python KIAkOAPI.

   b. Скрипты скачаны по ссылке https://box.kaspersky.com/d/579c0271a38e440b9144/ и размещены в директории /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts.

   c. Скрипты подключены к Kaspersky Security Center.

      Поскольку учетные данные не защищены, мы рекомендуем использовать отдельного пользователя Kaspersky Security Center, созданного в пункте 2, для подключения скриптов к Kaspersky Security Center, а также ограничить доступ к директории со скриптами. Для подключения следует открыть скрипты в режиме редактирования и оформить строки следующим образом:

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"
```

Настройка реагирования

Чтобы создать правило реагирования в коррелятоpe KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы и сервисы** → **Корреляторы** создайте коррелятор или откройте действующий коррелятор в режиме редактирования.

2. В мастере создания коррелятора на шаге **Реагирование** нажмите **Добавить правило реагирования** и в открывшемся окне **Реагирование** заполните следующие поля:

   a. В раскрывающемся списке **Тип** укажите тип правила реагирования **Запуск скрипта**.

   b. В поле **Время ожидания** укажите количество секунд, в течение которого должно завершиться выполнение скрипта. Если указанное значение будет превышено, выполнение скрипта прервется. Установите значение **600** (10 мин).

   c. В поле **Название скрипта** укажите название скрипта, например **deleteFile.py**.

   d. В поле **Аргументы скрипта** укажите параметры или значения полей событий, которые необходимо передать скрипту. Чтобы указывать неэкранированные символы в параметрах, используйте одинарные кавычки. Аргументы представлены для каждого скрипта в раскрывающихся блоках.

      onDemandScan.py – проверка важных областей

      Скрипт onDemandScan автоматически создает и запускает задачу *Проверка важных областей* при обнаружении определенных событий KUMA. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

      Ограничения

      Если у вас развернуто решение Kaspersky Sandbox или KATA Sandbox, после обновления плагина управления до версии 12.9 вам нужно переустановить фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Это нужно для обновления прав пользователей на новую функциональность поддержки EDR-действий по реагированию на угрозы для KUMA.

      Аргументы

      Для настройки задачи *Проверка важных областей* вам нужно задать следующие аргументы для скрипта:

      `--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--recursive true|false` – режим рекурсивной проверки. Введите этот аргумент вручную.

`--path` – список файлов и папок для выборочной проверки через пробел.

Вы также можете выбрать предустановленный области проверки. В Kaspersky Endpoint Security предустановлены следующие объекты для формирования области проверки:

- **Системная память**.
- **Запущенные процессы и объекты автозапуска**.

  Память, занятая процессами, и исполняемые файлы приложения, которые запускаются при старте операционной системы.
- **Загрузочные секторы**.

  Загрузочные секторы жестких и съемных дисков.
- **Системное резервное хранилище**.

  Содержимое папки System Volume Information.
- **Все внешние устройства**.
- **Все жесткие диски**.
- **Все сетевые диски**.

Для этого вам нужно в скрипте onDemandScan для параметра "enabled" соответствующей области проверки установить значение True или False:

```
defaultPreset = [
    {"enabled": False, "path": "%personal%", "recursive": True,
        "type": ScanObjectType.Folder.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.Email.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.SystemMemory.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.StartupObjectsAndRunningProcesses.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.DiskBootSectors.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.SystemBackupStorage.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllRemovableDrives.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllFixedDrives.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllNetworkDrives.value}
```

Пример

```
python3 onDemandScan.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --recurive
false --path 'C:\Program Files (x86)\Example Folder'
```

Скрипт onDemandScan автоматически создает и запускает задачу *Проверка важных областей* при обнаружении определенных событий KUMA. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Ограничения

Если у вас развернуто решение Kaspersky Sandbox или KATA Sandbox, после обновления плагина управления до версии 12.9 вам нужно переустановить фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Это нужно для обновления прав пользователей на новую функциональность поддержки EDR-действий по реагированию на угрозы для KUMA.

Аргументы

Для настройки задачи *Проверка важных областей* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--recursive true|false` – режим рекурсивной проверки. Введите этот аргумент вручную.

`--path` – список файлов и папок для выборочной проверки через пробел.

Вы также можете выбрать предустановленный области проверки. В Kaspersky Endpoint Security предустановлены следующие объекты для формирования области проверки:

- **Системная память**.
- **Запущенные процессы и объекты автозапуска**.

  Память, занятая процессами, и исполняемые файлы приложения, которые запускаются при старте операционной системы.
- **Загрузочные секторы**.

  Загрузочные секторы жестких и съемных дисков.
- **Системное резервное хранилище**.

  Содержимое папки System Volume Information.
- **Все внешние устройства**.
- **Все жесткие диски**.
- **Все сетевые диски**.

Для этого вам нужно в скрипте onDemandScan для параметра "enabled" соответствующей области проверки установить значение True или False:

```
defaultPreset = [
    {"enabled": False, "path": "%personal%", "recursive": True,
        "type": ScanObjectType.Folder.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.Email.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.SystemMemory.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.StartupObjectsAndRunningProcesses.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.DiskBootSectors.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.SystemBackupStorage.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllRemovableDrives.value},
```

```
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllFixedDrives.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllNetworkDrives.value}
```

Пример

```
python3 onDemandScan.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --recurive
false --path 'C:\Program Files (x86)\Example Folder'
```

ioCScan.py – поиск индикаторов компрометации

Скрипт iocScan автоматически создает и запускает задачу *Поиск IOC* при обнаружении определенных событий KUMA. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC.

Ограничения

По умолчанию Kaspersky Endpoint Security выполняет поиск IOC только в важных областях компьютера, таких как папки Загрузки, Рабочий стол, папка с временными файлами операционной системы и другие.

По умолчанию выбраны следующие журналы событий: журнал событий приложений, журнал системных событий и журнал событий безопасности.

Аргументы

Для настройки задачи *Поиск IOC* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--iocZip` – путь к ZIP-архиву с IOC-файлом в кодировке base64, по которым требуется выполнять поиск. Обязательный аргумент. Введите этот аргумент вручную.

`--isolateHost true|false` – изоляция компьютера от сети при обнаружении индикатора компрометации для предотвращения распространения угрозы. Обязательный аргумент. Введите этот аргумент вручную.

`--quarantineObject true|false` – удаление вредоносного объекта при обнаружении индикатора компрометации. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин. Обязательный аргумент. Введите этот аргумент вручную.

`--scanCriticalAreas true|false` – запуск задачи *Проверка важных областей* при обнаружении индикатора компрометации. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы. Обязательный аргумент. Введите этот аргумент вручную.

Пример

```
python3 iocScan.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --iocZip
'./ioc.zip' --isolateHost true --scanCriticalAreas true --quarantineObject true
```

quarantineFile.py – помещение файла на карантин

Скрипт quarantineFile автоматически создает и запускает задачу *Помещение файла на карантин* при получении в KUMA определенных событий. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

Ограничения

Задача *Помещение файла на карантин* имеет следующие ограничения:

1. Размер файла не должен превышать 100 МБ.
2. Файлы, необходимые для работы Kaspersky Endpoint Security for Linux, удалить невозможно:
   - файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security for Linux;
   - файлы, имеющие цифровую подпись "Лаборатории Касперского".

Аргументы

Для настройки задачи *Помещение файла на карантин* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--path` – путь к файлу. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--md5hash` – MD5-хеш файла. Скрипт получает этот аргумент из события.

`--sha256hash` – SHA256-хеш файла. Скрипт получает этот аргумент из события.

Примеры

```
python3 quarantineFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt'
```

```
python3 quarantineFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --sha256hash 1234567891012345678901234567890 12
```

deleteFile.py – удаление файла

Скрипт deleteFile автоматически создает и запускает задачу *Удаление файла* при обнаружении определенных событий KUMA. Например, вы можете удаленно удалить файл при реагировании на угрозы.

Ограничения

Файлы, необходимые для работы Kaspersky Endpoint Security for Linux, удалить невозможно:

- файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security for Linux;
- файлы, имеющие цифровую подпись "Лаборатории Касперского".

Аргументы

Для настройки задачи *Удаление файла* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--searchInSubfolders true|false` – поиск файла в подпапках. Обязательный аргумент. Введите этот аргумент вручную.

`--path` – путь к файлу. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--md5hash` – MD5-хеш файла. Скрипт получает этот аргумент из события.

`--sha256hash` – SHA256-хеш файла. Скрипт получает этот аргумент из события.

Примеры

```
python3 deleteFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt' --searchInFolders false
```

```
python3 deleteFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path '1' -
-searchInFolders false --sha256hash 1234567891012345678901234567890 12
```

getFile.py – получение файла

Скрипт getFile автоматически создает и запускает задачу *Получение файла* при получении в KUMA определенных событий. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. В результате выполнения задачи копия файла будет сохранена в карантине. *Карантин* – это специальное локальное хранилище на компьютере. Вы можете загрузить этот файл на компьютер из карантина в Web Console (**Операции** → **Хранилища** → **Карантин**). При этом на компьютере пользователя файл остается в исходной папке.

Ограничение

Размер файла не должен превышать 100 МБ.

Аргументы

Для настройки задачи *Получение файла* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--path` – путь к файлу. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--md5hash` – MD5-хеш файла. Скрипт получает этот аргумент из события.

`--sha256hash` – SHA256-хеш файла. Скрипт получает этот аргумент из события.

Примеры

```
python3 getFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt'
```

```
python3 getFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --md5hash 12345678910123456789012345678901 2
```

isolateHost.py – сетевая изоляция компьютера

Скрипт isolateHost автоматически изолирует компьютер из сети при обнаружении определенных событий KUMA.

После включения Сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на компьютере, кроме следующих соединений:

- соединения, указанные в исключениях из Сетевой изоляции;
- соединения, инициированные службами Kaspersky Endpoint Security;
- соединения, инициированные Агентом администрирования Kaspersky Security Center;
- соединения с SVM и Сервером интеграции, если приложение используется в режиме Легкого агента;
- соединения с KSN при интеграции приложения с Kaspersky Managed Detection and Response.

Аргументы

Для настройки Сетевой изоляции вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--action` – режим Сетевой изоляции. Обязательный аргумент. Введите этот аргумент вручную. Возможные значения:

- `1` – изолировать компьютер от сети;
- `0` – выключить Сетевую изоляцию.

Пример

```
python3 isolateHost.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --action 1
```

preventExecution.py – запрет запуска объектов

Скрипт preventExecution автоматически запрещает запуск объектов при обнаружении определенных событий KUMA. Запрет запуска объектов позволяет контролировать запуск исполняемых файлов и скриптов, а также открытие файлов офисного формата. Таким образом, вы можете, например, запретить запуск приложений, использование которых считаете небезопасным. В результате распространение угрозы может быть остановлено. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов. *Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

> Kaspersky Endpoint Security контролирует создание новых правил запрета запуска и игнорирует повторяющиеся правила. То есть, если запуск объекта уже запрещен, то приложение не будет создавать новое правило. При этом все параметры правила должны совпадать (путь до файла и хеш файла), и правило должно быть включено.

Ограничения

Запрет запуска объектов имеет следующие ограничения:

1. Правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Приложение не будет блокировать исполнение или открытие этих файлов.
2. Применить правило запрета к файлам, необходимым для работы Kaspersky Endpoint Security for Linux, невозможно:
   - файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security for Linux;
   - файлы, имеющие цифровую подпись "Лаборатории Касперского".
3. Не рекомендуется создавать более 5000 правил запрета запуска, поскольку это может привести к нестабильности системы.

Аргументы

Для настройки Запрета запуска объектов вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--hash` – MD5-хеш файла. Обязательный аргумент.Скрипт получает этот аргумент из события.

`--path` – полный путь к файлу или путь к файлу, если вы введете хеш файла. Обязательный аргумент. Скрипт получает этот аргумент из события.

Пример

```
python3 preventExecution.py --targetHost '422db51e-9383-46d4-b75d-f4d1d20fff2c' --
path 'C:\test5\run10.exe' --hash '8806b7f358884a049675b42c5f75ba10'
```

startProcess.py – запуск процесса

Скрипт startProcess автоматически создает и запускает задачу *Запуск процесса* при обнаружении определенных событий KUMA. Например, вы можете удаленно запускать утилиту, которая создает файл с конфигурацией компьютера. Далее с помощью задачи *Получение файла*, вы можете получить созданный файл в Kaspersky Security Center Web Console.

Аргументы

Для настройки задачи *Запуск процесса* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--executablePath` – путь к файлу. Обязательный аргумент. Вы можете передать этот аргумент из события или ввести значение вручную.

`--arguments` – дополнительные аргументы для запуска процесса. Введите эти аргументы вручную.

`--workingFolder` – путь к рабочей папке процесса. Введите этот аргумент вручную.

Пример

```
python3 startProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --
executablePath 'c://a/a.exe'
```

terminateProcess.py – завершение процесса

Скрипт terminateProcess автоматически создает и запускает задачу *Завершение процесса* при обнаружении определенных событий KUMA. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи *Запуск процесса*.

Если вы хотите запретить запуск файла, вы можете настроить компонент Запрет запуска объектов. Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Ограничения

Завершить процессы файлов, необходимых для работы Kaspersky Endpoint Security для Windows, невозможно:

- файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security для Windows;
- файлы, имеющие цифровую подпись "Лаборатории Касперского".

Аргументы

Для настройки задачи *Завершение процесса* вам нужно задать следующие аргументы для скрипта:

`--targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--caseSensitive true|false` – включение режима учета регистра при поиске файла. Обязательный аргумент. Введите этот аргумент вручную.

`--path` – путь к файлу. Обязательный аргумент. Скрипт получает этот аргумент из события.

`--md5hash` – MD5-хеш файла. Скрипт получает этот аргумент из события.

`--sha256hash` – SHA256-хеш файла. Скрипт получает этот аргумент из события.

Примеры

```
python3 terminateProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\file.exe' --caseSensitive true

python3 terminateProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --caseSensitive false --md5hash 12345678910123456789012345678901 2
```

e. В поле **Обработчики** укажите количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

f. При необходимости в поле **Описание** укажите произвольное описание правила реагирования.

g. В поле **Фильтр** определите условия, при соответствии которым события будут обрабатываться с применением правила реагирования.

3. Сохраните параметры и установите сервис коррелятора на сервере или перезапустите действующий коррелятор, чтобы применить параметры.

При получении корреляционного события с определенными полями будет срабатывать правило реагирования в KUMA, запускающее выполнение EDR-действия. В результате в Kaspersky Security Center будет создана и запущена соответствующая задача. Записи можно посмотреть в журналах Kaspersky Security Center и Kaspersky Endpoint Security.

Шаблоны уведомлений

Шаблоны уведомлений используются для создания уведомлений по электронной почте о событиях следующих типов:

- **Созданный алерт**.
- **Завершение генерации отчета**.
- **Завершение асинхронной задачи** (шаблон с таким типом может быть только один).
- **Нарушение политики мониторинга**.
- **Перемещение пользователя в другую группу KASAP**.

Вы можете создавать шаблоны всех типов событий для Общего тенанта. Для всех остальных тенантов доступны только типы событий **Созданный алерт** и **Нарушение политики мониторинга**.

Предустановленные шаблоны уведомлений

В поставку KUMA включены перечисленные в таблице ниже шаблоны уведомлений.

Предустановленные шаблоны уведомлений

Название шаблона	Описание
[OOTB] New alert in KUMA	Базовый шаблон уведомлений.

Создание шаблона уведомления

Чтобы создать шаблон уведомления:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Шаблоны уведомлений**.

   В правой части раздела **Ресурсы** отобразится таблица **Шаблоны уведомлений**.

2. Нажмите на кнопку **Добавить** и в открывшемся окне задайте параметры, как описано в таблице ниже.

Параметры шаблонов уведомлений

Параметр	Описание
Название	Обязательный параметр. Уникальное имя шаблона. Должно содержать от 1 до 128 символов в кодировке Unicode. Имя не должно начинаться и заканчиваться пробелом и не должно содержать управляющие последовательности (перевод строки и т.п.).
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс. Вы можете создавать шаблоны всех типов событий для Общего тенанта. Для всех остальных тенантов доступны только типы **Созданный алерт** и **Нарушение политики мониторинга**.
Тип	Обязательный параметр. Тип события, для которого необходимо создать шаблон уведомления. Доступны следующие типы: • **Созданный алерт**. • **Завершение генерации отчета**. • **Завершение асинхронной задачи**. Шаблон с таким типом может быть только один. Если шаблон с таким типом уже существует, этот тип будет недоступен для выбора при создании нового шаблона. • **Нарушение политики мониторинга**. • **Перемещение пользователя в другую группу KASAP**.
Тема	Обязательный параметр. Тема электронного письма с уведомлением. Максимальная длина поля – 140 символов в кодировке Unicode. Текст необходимо указывать на русском или английском языке в зависимости от локализации, выбранной в профиле пользователя. Для каждого типа событий при создании шаблона доступен стандартный текст темы. Поле **Тема** недоступно для редактирования или выбора стандартного текста, пока не выбран тип шаблона в поле **Тип**. В теме письма можно обращаться к полям объектов в зависимости от выбранного типа события. Пример (тема в шаблоне уведомления для события типа **Созданный алерт**): `Новый алерт в KUMA: {{.CorrelationRuleName}}`. Вместо `{{.CorrelationRuleName}}` в теме письма с уведомлением будет подставлено название правила корреляции, содержащееся в поле алерта `CorrelationRuleName`.
Шаблон	Обязательный параметр. Тело электронного письма с уведомлением. Текст необходимо указывать на русском или английском языке в зависимости от локализации, выбранной в профиле пользователя. Шаблон поддерживает синтаксис, с помощью которого уведомление можно динамически наполнить данными из указанных полей соответствующих объектов. Описание синтаксиса шаблонов уведомлений и список поддерживаемых полей вы можете найти в статье Синтаксис шаблонов уведомлений. Для каждого типа событий при создании шаблона доступен стандартный текст электронного письма. Для удобства текст письма можно открыть в отдельном окне, нажав на значок . При этом открывается окно **Шаблон**, в котором можно изменить текст письма с уведомлением. Сохранить изменения и закрыть окно можно с помощью кнопки **OK**.
По умолчанию	Необязательный параметр. Доступен для типа событий **Завершение асинхронной задачи**. Если флажок установлен, то создаваемый шаблон применяется вместо системного шаблона ко всем задачам, созданным после сохранения шаблона.

Параметр	Описание
Теги	Необязательный параметр. Теги для создаваемого шаблона уведомления. 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.
Описание	Необязательный параметр. Описание шаблона в виде произвольного текста. Максимальная длина до 4000 символов в кодировке Unicode.

3. Нажмите **Сохранить**.

Шаблон уведомления создан и отображается в таблице **Шаблоны уведомлений**.

Изменение шаблона уведомления

Чтобы изменить шаблон уведомления:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Шаблоны уведомлений**.

   В правой части раздела **Ресурсы** отобразится таблица **Шаблоны уведомлений**.

2. Откройте нужный шаблон нажатием на соответствующую строку в таблице, и в открывшемся окне измените параметры, перечисленные в таблице в статье Создание шаблона уведомления.

3. Нажмите **Сохранить**.

Шаблон уведомления изменен.

Удаление шаблона уведомления

Чтобы удалить шаблон уведомления:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Шаблоны уведомлений**.

   В правой части раздела **Ресурсы** отобразится таблица **Шаблоны уведомлений**.

2. Установите флажки рядом с шаблонами уведомлений, которые вы хотите удалить.

   Если вы хотите удалить все существующие шаблоны, нажмите на флажок рядом со столбцом **Название** и выберите в раскрывающемся списке **Выбрать все**.

   Если вы хотите удалить все шаблоны, отображающиеся на странице, нажмите на флажок рядом со столбцом **Название** и выберите в раскрывающемся списке **Выбрать все на странице**.

   Необходимо установить хотя бы один флажок.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения. Если среди удаляемых шаблонов есть шаблоны, связанные с других другими ресурсами или сервисами, они будут показаны в окне подтверждения с примечанием, что эти шаблоны не будут удалены.

4. Нажмите на кнопку **Удалить**, чтобы подтвердить удаление.

Шаблоны, для которых возможно безопасное удаление, будут удалены.

Синтаксис шаблонов уведомлений

В шаблонах уведомлений используется синтаксис Go templates. С помощью этого синтаксиса можно динамически наполнять содержимым уведомления: загружать данные из полей соответствующих объектов, вставлять ссылки или преобразовывать даты в нужный формат. Синтаксис шаблонов можно использовать как в теме письма, так и в теле сообщения. В этой статье дается краткая информация о синтаксисе, а также перечислены поля, которые можно использовать для тех или иных типов событий, и дополнительные функции, применяемые к этим полям. Подробнее про синтаксис вы можете прочитать в официальной документации языка Go.

В шаблоне можно обращаться к полям объектов в зависимости от выбранного типа событий. Поля соответствующих объектов могут содержать простые значения, такие как строка или число:

```
{{ .CorrelationRuleName }}
```

В письме будет отображаться название алерта, то есть содержимое поля `CorrelationRuleName` модели данных алерта.

Некоторые поля могут содержать содержат массивы данных, например поля алерта с относящимися к нему событиями, активами, учетными записями. К таким вложенным объектам можно обращаться с помощью функции `range`, которая последовательно обращается к полям 50 первых вложенных объектов. При обращении с помощью функции `range` к полю, в котором нет массива данных, возвращается ошибка. Пример:

```
{{ range .Assets }}
Устройство: {{ .DisplayName }}, дата создания: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DeviceHostName` и `CreatedAt` из 50 связанных с алертом активов:

```
Устройство: <значение поля DisplayName из актива 1>, дата создания: <значение поля CreatedAt из актива 1>
Устройство: <значение поля DisplayName из актива 2>, дата создания: <значение поля CreatedAt из актива 2>
...
// Всего 50 строк
```

С помощью функции `limit` можно ограничить количество объектов, возвращаемых функцией `range`:

```
{{ range (limit .Assets 5) }}
<strong>Устройство</strong>: {{ .DisplayName }},
<strong>Дата создания</strong>: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DisplayName` и `CreatedAt` из 5 связанных с алертом активов, слова "Устройства" и "Дата создания" выделены HTML-тегами `<strong>`:

```
<strong>Устройство</strong>:  <значение поля DeviceHostName из актива 1>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива 1>
<strong>Устройство</strong>: <значение поля DeviceHostName из актива N>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива N>
...
// Всего 10 строк
```

Вложенные объекты могут иметь свои вложенные объекты. К ним можно обратиться с помощью вложенных функций `range`:

```
{{ range (limit .Events 5) }}
    {{ range (limit .Event.BaseEvents 10) }}
    Идентификатор сервиса: {{ .ServiceID }}
    {{ end }}
{{ end }}
```

В письме будет отображаться по десять идентификаторов сервисов (поле `ServiceID`) из базовых событий, относящихся к пяти корреляционным событиям алерта (всего 50 строк). Обратите внимание, что обращение к событиям происходит через вложенную структуру `EventWrapper`, которая находится в алерте в поле `Events`. События доступны в поле `Event` этой структуры, что отражено в примере выше. Таким образом, если поле `A` содержит вложенную структуру `[B]` и в структуре `[B]` есть поле `C`, которое является строкой или числом, то чтобы обратиться к полю `C`, необходимо указать путь `{{ A.C }}`.

Некоторые поля объектов содержат вложенные словари в формате "ключ – значение" (например, поле событий `Extra`). К ним можно обратиться с помощью функции `range` с переданными ей переменными: `range $placeholder1, $placeholder2 := .FieldName`. Значения переменных затем можно вызывать, указывая из названия. Пример:

```
{{ range (limit .Events 3) }}
    {{ range (limit .Event.BaseEvents 5) }}
    Список полей в поле события Extra: {{ range $name, $value := .Extra }} {{ $name }} - {{ $value }} <br> {{ end
}}
    {{ end }}
{{ end }}
```

В письме через HTML-тег
 будут отображаться пары "ключ – значение" из полей `Extra` базовых событий, принадлежащих корреляционным событиям. Вызываются данные из пяти базовых событий из каждого из трех корреляционных событий.

В шаблонах уведомлений можно использовать HTML-теги, выстраивая их в сложные структуры. Пример таблицы для полей корреляционного события:

```
<style type="text/css">
  TD, TH {
    padding: 3px;
    border: 1px solid black;
  }
</style>
<table>
  <thead>
    <tr>
        <th>Название сервиса</th>
        <th>Название корреляционного правила</th>
        <th>Версия устройства</th>
    </tr>
  </thead>
  <tbody>
    {{ range .Events }}
    <tr>
        <td>{{ .Event.ServiceName }}</td>
        <td>{{ .Event.CorrelationRuleName }}</td>
        <td>{{ .Event.DeviceVersion }}</td>
    </tr>
    {{ end }}
  </tbody>
</table>
```

С помощью функции **link_alert** в письмо с уведомлением можно вставить HTML-ссылку на алерт:

```
{{link_alert}}
```

В письме будет отображаться ссылка на окно алерта.

Шаблоны также поддерживают более сложные конструкции, такие как объявление локальных переменных, использование операторов сравнения и управляющих структур. Ниже приведен пример, как можно из связанных с алертом данных извлечь сведения о наивысшей категории активов и поместить ее в уведомления:

```
{{ $criticalCategoryName := "" }}
{{ $maxCategoryWeight := 0 }}
{{ range .Assets }}
    {{ range .CategoryModels }}
        {{ if gt .Weight $maxCategoryWeight }}
            {{ $maxCategoryWeight = .Weight }}
            {{ $criticalCategoryName = .Name }}
        {{ end }}
    {{ end }}
{{ end }}
{{ if gt $maxCategoryWeight 1 }}
Наивысшая категория активов: {{ $criticalCategoryName }}
{{ end }}
```

Поля объектов, поддерживаемые в шаблонах

В таблице ниже перечислены поля, к которым можно обращаться из шаблонов в зависимости от типа события.

Поддерживаемые поля объектов

Тип	Доступные поля
Созданный алерт	Поддерживается обращение ко всем полям модели данных алерта, включая вложенные массивы и структуры.

Завершение генерации отчета	`{{ .Tenants }}` – тенанты, по которым построен отчет. `{{ .Name }}` – название отчета. `{{ .StartTime }}` – начало периода, за который строится отчет, в формате 2006-01-02 15:04:05 MSK. `{{ .FinishTime }}` – окончание периода, за который строится отчет, в формате 2006-01-02 15:04:05 MSK. `{{ .PreviewLink }}` – ссылка для просмотра отчета. `{{ .DownloadLink }}` – ссылка для скачивания отчета. Пример добавления ссылок в шаблон уведомления о генерации отчета: `Вы можете <a href="{{ .PreviewLink }}" target="_blank">просмотреть</a> или <a href="{{ .DownloadLink }}" target="_blank">скачать</a> отчет.`
Завершение асинхронной задачи	`{{ .Tenants }}` – тенант, в котором запущена задача. `{{ .TaskKind }}` – название задачи. `{{ .TaskCreator }}` – имя пользователя, который создал задачу (логин). `{{ .StartTime }}` – время начала выполнения задачи в формате 2006-01-02 15:04:05 MSK. `{{ .FinishTime }}` – время окончания выполнения задачи в формате 2006-01-02 15:04:05 MSK. `{{ .TaskStatus}}` – статус выполнения задачи.
Нарушение политики мониторинга	`{{ .SourceTenantName }}` – тенант источника событий. `{{ .SourceDisplayName }}` – имя источника. `{{ .Value }}` – значение, вышедшее за границы политики мониторинга на момент создания алерта. `{{ .WebLink }}` – ссылка на веб-интерфейс KUMA. `{{ .AlertActiveAt }}` – время, в которое был активен алерт. `{{ .PolicyName }}` – название политики мониторинга. `{{ .PolicyTenantName }}` – тенант политики мониторинга. `{{ .PolicyLowerEventBound }}` – нижний порог. `{{ .PolicyUpperEventBound }}` – верхний порог. `{{ .PolicyKind }}` – тип политики. `{{ .PolicyInterval }}` – интервал периода подсчета. `{{ .DeviceProduct }}` – устройство источника. `{{ .DeviceHostName }}` – имя хоста источника. `{{ .DeviceAddress }}` – адрес источника. `{{ .DeviceProcessName }}` – название процесса источника.
Перемещение пользователя в другую группу KASAP	`{{ .UserEmail }}` – отображаемое имя пользователя из Active Directory. `{{ .PreviousGroup}}` – группа обучения KASAP, в которой пользователь состоял на момент открытия его карточки из инцидента или алерта. `{{ .CurrentGroup}}` – группа обучения KASAP, в которую пользователь был перемещен из карточки пользователя. `{{ .WebLink }}` – ссылка на веб-интерфейс KUMA.

Функции в шаблонах уведомлений

В шаблонах доступны функции, перечисленные в таблице ниже.

Функция	Описание
`date`	Принимает первым параметром время в миллисекундах (unix time), вторым параметром можно передать формат времени по стандартам RFC. Часовой пояс изменить невозможно. Пример вызова: `{{ date .FirstSeen "02 Jan 06 15:04" }}` Результат вызова: 18 Nov 2022 13:46 Примеры форматов дат, поддерживаемые функцией: • `"02 Jan 06 15:04 MST"` • `"02 Jan 06 15:04 -0700"` • `"Monday, 02-Jan-06 15:04:05 MST"` • `"Mon, 02 Jan 2006 15:04:05 MST"` • `"Mon, 02 Jan 2006 15:04:05 -0700"` • `"2006-01-02T15:04:05Z07:00"`
`range`	Позволяет перебирать массивы или наборы пар "ключ – значение", последовательно обращаясь к полям 50 первых элементов.

`limit`	Функция вызывается внутри функции `range` для ограничения списка данных. Обрабатывает списки, которые не имеют ключей, принимает любой список данных первым параметром и обрезает список по второму значению. Например, в функцию можно передавать поля алерта `.Events`, `.Assets`, `.Accounts`, `.Actions`.
	Пример вызова:
	`{{ range (limit .Assets 5) }}`
	`<strong>Устройство</strong>: {{ .DisplayName }},`
	`<strong>Дата создания</strong>: {{ .CreatedAt }}`
	`{{ end }}`

`link_alert`	Формирует ссылку на алерт с URL, указанным в параметрах подключения к SMTP-серверу в качестве псевдонима сервера Ядра KUMA или с реальным URL сервиса Ядра KUMA, если псевдоним не задан. Пример вызова: `Подробнее об алерте можно узнать в веб-интерфейсе KUMA: {{link_alert}}.`

`link_task`	Формирует ссылку на задачу в KUMA.
	Пример вызова:
	`Задача "{{ .TaskKind }}" создана {{ .TaskCreator }} в {{ .StartTime }} и завершена в {{ .FinishTime }} со статусом "{{ .TaskStatus }}".`
	`Подробнее о задачах можно узнать в веб-интерфейсе KUMA: {{ link_task }}.`

`link`	Принимает вид ссылки, доступной для перехода. Пример вызова: `{{ link "https://support.kaspersky.com/KUMA/2.1/ru-RU/233508.htm" }}`

Коннекторы

Коннекторы используются для установления соединений между сервисами KUMA, а также для активного и пассивного получения событий.

Вы можете указать параметры коннекторов на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора.

Существуют следующие типы коннекторов:

- internal – используются для приема данных от сервисов KUMA по протоколу internal.
- tcp – используются для пассивного получения событий по протоколу TCP при работе с агентами Windows и Linux.
- udp – используются для пассивного получения событий по протоколу UDP при работе с агентами Windows и Linux.

- netflow – используются для пассивного получения событий в формате NetFlow.
- sflow – используются для пассивного получения событий в формате sFlow. Для sFlow поддерживаются только структуры, описанные в sFlow version 5.
- nats-jetstream – используются для взаимодействия с брокером сообщений NATS при работе с агентами Windows и Linux.
- kafka – используются для коммуникации с шиной данных Apache Kafka при работе с агентами Windows и Linux.
- http – используются для получения событий по протоколу HTTP при работе с агентами Windows и Linux.

sql – используются для выборки данных из СУБД. KUMA поддерживает работу с несколькими типами баз данных.

Поддерживаемые типы баз данных

Решение поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MariaDB 10.5 и выше.
- MsSQL.
- MySQL 5.7 и выше.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.
- При создании коннектора с типом **sql** вам нужно указать значения для общих параметров коннектора и отдельных параметров подключения к базе данных.
- file – используются для получения данных из текстовых файлов при работе с агентами Windows и Linux. Одна строка текстового файла считается одним событием. В качестве разделителя строк используется `\n`.
- 1c-log – используются для получения данных из технологических журналов программы 1С при работе с агентами Linux. В качестве разделителя строк используется `\n`. Из многострочной записи о событии коннектор принимает только первую строку.
- 1c-xml – используются для получения данных из журналов регистрации программы 1С при работе с агентами Linux. При обработке коннектором многострочные события преобразовываются в однострочные.
- diode – используются для однонаправленной передачи данных в промышленных ICS-сетях с помощью диода данных.
- ftp – используются для получения данных по протоколу File Transfer Protocol при работе с агентами Windows и Linux.

- nfs – используются для получения данных по протоколу Network File System при работе с агентами Windows и Linux.
- wmi – используются для получения данных с помощью Windows Management Instrumentation при работе с агентами Windows.
- wec – используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС хоста под управлением Windows при работе с агентами Windows.
- etw – используются для получения расширенных журналов DNS-серверов.
- snmp – используются для получения данных с помощью Simple Network Management Protocol при работе с агентами Windows и Linux. Для обработки событий, полученных по протоколу SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:
  - snmpV1;
  - snmpV2;
  - snmpV3.
- snmp-trap – используются для пассивного приема событий с помощью ловушек SNMP (англ. SNMP traps) при работе с агентами Windows и Linux. В коннекторе события snmp-trap принимаются и подготавливаются к нормализации путем сопоставления идентификаторов SNMP-объектов с временными ключами. Затем сообщение необходимо передать в JSON-нормализатор, где временные ключи будут сопоставлены с полями KUMA и будет создано событие. Для обработки событий, полученных по SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:
  - snmpV1;
  - snmpV2.
- kata/edr – используются для получения данных KEDR по API.
- vmware – используются для получения данных VMware vCenter по API.
- elastic – используются для получения данных Elasticsearch. Поддерживается работа с Elasticsearch версии 7.0.0.
- office365 – используются для получения данных Microsoft 365 (Office 365) по API.
- dfi – используются для получения данных Kaspersky Digital Footprint Intelligence по API.
- universalAPI – используются для получения данных из любых REST API, поддерживающих ответы в формате JSON. Поддерживается фильтрация по уникальному идентификатору и режим итераций.

Некоторые типы коннекторов (например, tcp, sql, wmi, wec и etw) поддерживают шифрование с использованием протокола TLS. KUMA поддерживает протокол TLS версии 1.2 или 1.3. При включении режима TLS для этих коннекторов подключение осуществляется по следующему алгоритму:

- Если KUMA используется в качестве клиента:
  1. KUMA отправляет запрос на соединение с сервером с максимальной поддерживаемой версией протокола TLS 1.3 ClientHello, а также список поддерживаемых криптонаборов.
  2. Сервер отвечает на запрос выбранной версией протокола TLS и криптонабора.
  3. В зависимости от версии протокола TLS в ответе сервера:
     - Если сервер отвечает на запрос, используя TLS 1.3 или 1.2, KUMA установит соединение с сервером.
     - Если сервер отвечает на запрос, используя TLS 1.1, KUMA закроет соединение с сервером.
- Если KUMA используется в качестве сервера:
  1. Клиент отправляет запрос на соединение с KUMA с максимальной поддерживаемой версией протокола TLS, а также список поддерживаемых криптонаборов.
  2. В зависимости от версии протокола TLS в запросе клиента:
     - Если в запросе клиента используется протокол TLS 1.1 ClientHello, KUMA закроет соединение.
     - Если в запросе клиента используется протокол TLS 1.2 или 1.3, KUMA ответит на запрос выбранной версией протокола TLS и криптонабора.

Просмотр параметров коннектора

Чтобы просмотреть параметры коннектора:

1. В веб-интерфейсе KUMA перейдите в раздел **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 веб-интерфейсе KUMA перейдите в раздел **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.

Коннектор, тип internal

Коннекторы с типом **internal** используются для приема данных от сервисов KUMA по протоколу internal. Например, такой коннектор должен быть использован для приема следующих данных:

- Внутренние данные, такие как маршруты событий.

- Файловые атрибуты. Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом file, 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.

  Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.

- События в маршрутизатор событий. Маршрутизатор событий может принимать события только по протоколу internal, поэтому при отправке событий в маршрутизатор событий вы можете использовать только точки назначения с типом **internal**.

Доступные параметры коннектора с типом **internal** 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.
Тип	Тип коннектора – **internal**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес и номер порта, который прослушивает коннектор. Вы можете ввести значение в одном из следующих форматов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `:< номер порта >`. IPv6-адреса можно указать в формате `[< IPv6-адрес >%< интерфейс >:< номер порта >`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Можно добавить только один URL-адрес. Если значение поля содержит пробелы или символы табуляции, невозможно сохранить ресурс или сервис. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Коннектор, тип tcp

Коннекторы с типом **tcp** используются для пассивного получения событий по протоколу TCP при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **tcp** 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.
Тип	Тип коннектора – **tcp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >:< номер порта >`; • `:< номер порта >`. Обязательный параметр.

Параметр	Описание
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно с auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для м auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся сп **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. KUMA классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие запис `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет исп префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F7` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.5 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid= pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:1206` поскольку они не передают важной для событий информации.
Разделитель	• **\n** (используется по умолчанию); • **\t**; • **\0**.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор KUMA и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 50 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором KUMA. Вы можете просмотреть в метриках KUMA, сколько оперативной памяти сервера использует коллектор KUMA. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором KUMA.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.

Параметр	Описание
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 решения и помещаются на сервер Ядра KUMA в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях KUMA. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

Коннектор, тип udp

Коннекторы с типом **upd** используются для пассивного получения событий по протоколу UDP при работе с агентами Windows и Linux. Доступные параметры коннектора 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.
Тип	Тип коннектора – **udp**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >:< номер порта >`; • `:< номер порта >`. Обязательный параметр.
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно с auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для м auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся с **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. KUMA классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие запис `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет исп префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F7` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.5 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid= pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:1206` поскольку они не передают важной для событий информации.
Разделитель	Символ, определяющий границу между событиями: • \n; • \t; • \0. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. Это значит, что не будет парсить одно событие на несколько, а передаст в нормализатор как есть.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор KUMA и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 50 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором KUMA. Вы можете просмотреть в метриках KUMA, сколько оперативной памяти сервера использует коллектор KUMA. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором KUMA.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

Коннектор, тип netflow

Коннекторы с типом **netflow** используются для пассивного получения событий в формате NetFlow. Доступные параметры коннектора с типом **netflow** 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.
Тип	Тип коннектора – **netflow**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный 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.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип sflow

Коннекторы с типом **sflow** используются для пассивного получения событий в формате sFlow. Для sFlow поддерживаются только структуры, описанные в sFlow version 5. Доступные параметры коннектора с типом **sflow** 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.
Тип	Тип коннектора – **sflow**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >:< номер порта >`; • `:< номер порта >`. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип nats-jetstream

Коннекторы с типом **nats-jetstream** используются для взаимодействия с брокером сообщений NATS при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **nats-jetstream** 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.
Тип	Тип коннектора – **nats-jetstream**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный 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.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша . **Как создать 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**.
Тема	Тема сообщений NATS. Символы вводятся в кодировке Unicode. Обязательный параметр.
Идентификатор группы	Значение параметра `GroupID` для сообщений NATS. Максимальная длина значения: до 255 символов в кодировке Unicode. Значение по умолчанию: `default`.
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.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание

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.
	
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать 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**.
	
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

Коннектор, тип kafka

Коннекторы с типом **kafka** используются для коммуникации с шиной данных Apache Kafka при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **kafka** описаны в таблицах ниже.

С помощью коннектора типа **kafka** KUMA может принимать события как в несжатом, так и в сжатом виде. Сжатие осуществляется с помощью следующих поддерживаемых **kafka** алгоритмов сжатия: gzip, snappy, zstd и lz4. При поступлении событий в сжатом виде декомпрессия событий происходит автоматически.

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.
Тип	Тип коннектора – **kafka**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный 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.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. • **PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать файл PFX из хранилища, после чего загрузить файл PFX в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. Если для проверки сервера используется цепочка из нескольких сертификатов, для обеспечения правильной очередности сертификатов в цепочке мы рекомендуем собирать файл PFX с помощью OpenSSL. • **SCRAM-SHA-256** – авторизация с помощью защищенного механизма подключения, который использует хеш SHA256 для безопасной проверки подлинности и предотвращает перехват данных. • **SCRAM-SHA-512** – авторизация с помощью защищенного механизма подключения, который использует хеш SHA512 для безопасной проверки подлинности и предотвращает перехват данных. При выборе **SCRAM-SHA-256** или **SCRAM-SHA-512** в качестве типа авторизации в раскрывающемся списке **Секрет** укажите секрет с паролем для авторизации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета в раскрывающемся списке **Секрет** выберите значение **Создать**.
Топик	Тема сообщений Kafka. Максимальная длина сообщения составляет 255 символов. Недопустимо использование символов пробела и табуляции. Вы можете использовать следующие символы: a–z, A–Z, 0–9, ".", "_", "-". Обязательный параметр.
Идентификатор группы	Значение параметра `GroupID` для сообщений Kafka. Максимальная длина значения: 255 символов. Вы можете использовать символы a–z, A–Z, 0–9, ".", "_", "-".
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.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999. По умолчанию количество обработчиков равно 256.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

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.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Размер одного сообщения в запросе	Размер одного сообщения в запросе в байтах. Значение по умолчанию: 16 МБ, применяется если значение не указано или указано 0. Значение не может быть больше 2147483647 байт.
Максимальное время ожидания одного сообщения	Время ожидания одного сообщения в секундах. Значение по умолчанию: 5 секунд, применяется если значение не указано или указано 0. Максимально допустимое значение= 2147483647.
Время ожидания подключения	Время ожидания установки соединения с брокером Kafka в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания чтения	Время ожидания операции чтения в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания записи	Время ожидания операции записи в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.

Параметр	Описание
Интервал обновления состояния группы	Интервал обновления состояния группы в секундах. Интервал обновления не может превышать время сессии. Рекомендуемое значение: 1/3 от времени сессии. Максимально допустимое значение: 2147483647. По умолчанию 3 секунды.
Время сессии	Время сессии в секундах. Максимально допустимое значение: 2147483647. По умолчанию 10 секунд.
Максимальное время обработки одного сообщения	Максимальное время обработки одного сообщения одним потоком в миллисекундах. Максимально допустимое значение: 2147483647. По умолчанию 100 миллисекунд.
Включить автокоммит	По умолчанию включено.
Интервал автокоммита	Интервал автокоммита в секундах. По умолчанию 1 секунда. Максимально допустимое значение: 18446744073709551615. Можно указать любое положительное число.

Коннектор, тип http

Коннекторы с типом **http** используются для получения событий по протоколу HTTP при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **http** описаны в таблицах ниже.

С помощью коннектора типа **http** KUMA может принимать события как в несжатом, так и в сжатом виде. При поступлении событий в сжатом виде, например событий Kaspersky Endpoint Security for Windows, декомпрессия событий происходит автоматически.

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.
Тип	Тип коннектора – **http**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >:< номер порта >`; • `:< номер порта >`. Для того чтобы данные из источника событий отправлялись в коннектор, указанный вами URL-адрес должен оканчиваться на `/input`. Обязательный параметр.

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.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
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 решения и помещаются на сервер Ядра KUMA в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях KUMA. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение Создать. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение Создать. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**.

Коннектор, тип sql

Коннекторы с типом **sql** используются для выборки данных из СУБД. KUMA поддерживает работу с несколькими типами баз данных.

Поддерживаемые типы баз данных

Решение поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MariaDB 10.5 и выше.
- MsSQL.
- MySQL 5.7 и выше.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.

При создании коннектора с типом **sql** вам нужно указать значения для общих параметров коннектора и отдельных параметров подключения к базе данных. Доступные параметры коннектора с типом **sql** 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.
Тип	Тип коннектора – **sql**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Запрос по умолчанию	SQL-запрос, который выполняется при подключении к базе данных. Обязательный параметр.
Переподключаться к БД каждый раз при отправке запроса	Переключатель, включающий переключение коннектора к базе данных при отправке запроса. По умолчанию этот переключатель выключен.
Интервал запросов, сек.	Интервал выполнения SQL-запросов в секундах. Значение по умолчанию: 10 секунд.

<table>
<tr><th>Параметр</th><th>Описание</th></tr>
<tr><td>Соединение</td><td>
Параметры в этом блоке зависят от выбранного типа базы данных для подключения:
MySQL
Postgres
SQLite3
Oracle
Firebird
ClickHouse
ODBC

Тип базы данных – тип базы данных для подключения. При выборе типа базы данных в поле URL отображается префикс, соответствующий протоколу взаимодействия. Например, для типа базы данных ClickHouse в поле URL отображается префикс <code>clickhouse://</code>.
Секрет отдельно – флажок, позволяющий просматривать информацию о подключении.
URL – URL-адрес подключения. Вы сможете просматривать информацию о подключении и вам не придется повторно создавать большое количество подключений при изменении пароля учетной записи, которую вы использовали для подключений.
При создании подключений, если информация о подключении задана в URL-адресе, могут неправильно обрабатываться строки с учетными данными, содержащими специальные символы. Если при создании подключения возникает ошибка, но вы уверены в том, что указали правильные значения параметров, укажите специальные символы в процентной кодировке.
Коды специальных символов
<table>
<tr><td>!</td><td>#</td><td>$</td><td>%</td><td>&</td><td>'</td><td>(</td><td>)</td><td>*</td><td>+</td></tr>
<tr><td>%21</td><td>%23</td><td>%24</td><td>%25</td><td>%26</td><td>%27</td><td>%28</td><td>%29</td><td>%2A</td><td>%2B</td></tr>
<tr><td>,</td><td>/</td><td>:</td><td>;</td><td>=</td><td>?</td><td>@</td><td>[</td><td>]</td><td>\</td></tr>
<tr><td>%2C</td><td>%2F</td><td>%3A</td><td>%3B</td><td>%3D</td><td>%3F</td><td>%40</td><td>%5B</td><td>%5D</td><td>%5C</td></tr>
</table>
Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.
Если вы установили флажок Секрет отдельно, учетные данные задаются в секрете и кодируются автоматически. В этом случае кодирование специальных символов не требуется.
В раскрывающемся списке Брать URL из секрета вы можете выбрать существующий URL-адрес или создать новый URL-адрес. Для создания нового URL-адреса нажмите Создать.
Если вы хотите изменить параметры существующего URL-адреса, нажмите рядом с ним на значок карандаша 🖉.
Секрет – секрет urls, в котором хранится список URL-адресов для подключения к базе данных. Это поле отображается, если вы установили флажок Секрет отдельно.
Столбец идентификатора – название столбца, содержащего идентификатор для каждой строки таблицы. Обязательный параметр.
Начальное значение идентификатора – значение в столбце идентификатора для определения строки, с которой требуется начать считывание данных из SQL-таблицы.
Запрос – дополнительный SQL-запрос, который выполняется вместо SQL-запроса по умолчанию.
Интервал запросов, сек – интервал выполнения SQL-запросов в секундах. Указанный интервал используется вместо интервала, указанного по умолчанию для коннектора. Значение по умолчанию: 10 секунд.

Вы можете добавить несколько подключений или удалить подключение. Для добавления подключения нажмите на кнопку + Добавить подключение. Для удаления подключения нажмите рядом с ним на значок удаления ✕.
</td></tr>
<tr><td>Описание</td><td>Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.</td></tr>
</table>

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**. KUMA конвертирует ответы SQL в кодировку UTF-8. Вы можете настроить SQL-сервер на отправку ответов в кодировке UTF-8 или выбрать их кодировку на стороне KUMA.

В рамках одного коннектора вы можете **создать подключение** для нескольких поддерживаемых баз данных. Если коллектор с коннектором типа **sql** не удается запустить, вам нужно проверить, пуст ли state-файл /opt/kaspersky/kuma/collector/<`идентификатор коллектора`>/sql/state-<`идентификатор файла`>. Если state-файл пуст, вам нужно его удалить и перезапустить коллектор.

Чтобы создать подключение для нескольких баз данных SQL:

1. Нажмите на кнопку **Добавить подключение**.
2. Задайте значение для параметров **URL**, **Столбец идентификатора**, **Начальное значение идентификатора**, **Запрос**, **Интервал запросов, сек**.
3. Повторите шаги 1–2 для каждого требуемого подключения.

Поддерживаемые типы SQL и особенности их использования

Поддерживаются следующие типы SQL:

- MSSQL.

  Например:

  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}`

  Мы рекомендуем использовать этот вариант URL.

  - `sqlserver://{user}:{password}@{server}?database={database}`

  В качестве плейсхолдера в SQL-запросе используются символы `@p1`.

  > Если вы хотите подключиться с доменными учетными данными, укажите имя учетной записи в формате < домен >%5C< пользователь >. Например: `sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`.

- MySQL/MariaDB.

  Например:

  `mysql://{user}:{password}@tcp({server}:{port})/{database}`

  В качестве плейсхолдера в SQL-запросе используются символ `?`.

- PostgreSQL.

  Например: `postgres://{user}:{password}@{server}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- CockroachDB.

  Например:

  `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- SQLite3.

  Например:

  `sqlite3://file:{file_path}`

В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

При обращении к SQLite3, если начальное значение идентификатора используется в формате datetime, вам нужно добавить преобразование даты с помощью функции `sqlite datetime` в SQL-запрос. Например:

```
select * from connections where datetime(login_time) > datetime(?, 'utc') order by
login_time
```

В этом примере `connections` – это таблица SQLite, а значение переменной `?` берется из поля **Начальное значение идентификатора**, и его требуется указывать в формате `{< дата >}T{< время >}Z`, например `2021-01-01T00:10:00Z)`.

- Oracle DB.

  Пример URL секрета с драйвером oracle:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}
  ```

  ```
  oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}
  ```

  Если время выполнения запроса превышает 30 секунд. драйвер oracle прерывает SQL-запрос и в журнале коллектора появится ошибка **user requested cancel of current operation**. Для увеличения времени выполнения SQL-запроса укажите в строке подключения значение параметра **timeout** в секундах, например:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}?timeout=300
  ```

  В качестве плейсхолдера в SQL-запросе используется переменная `:val`.

  При обращении к Oracle DB, если начальное значение идентификатора используется в формате datetime, требуется учитывать тип поля в базе данных и при необходимости добавить дополнительные преобразования строки со временем в SQL-запросе для обеспечения правильной работы SQL-коннектора. Например, если в базе создана таблица `Connections`, в которой есть поле `login_time`, возможны следующие преобразования:

  - Если у поля **login_time** тип TIMESTAMP, в зависимости от параметров базы данных в поле **login_time** может быть указано значение в формате `YYYY-MM-DD HH24:MI:SS`, например `2021-01-01 00:00:00`. В этом случае вам нужно указать значение `2021-01-01T00:00:00Z` в поле **Начальное значение идентификатора**, а в SQL-запросе произвести преобразование с помощью функции `to_timestamp`, например:

    ```
    select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-
    DD"T"HH24:MI:SS"Z"')
    ```

  - Если у поля **login_time** тип TIMESTAMP WITH TIME ZONE, в зависимости от параметров базы данных в поле **login_time** может быть указано значение в формате `YYYY-MM-DD"T"HH24:MI:SSTZH:TZM`, например `2021-01-01T00:00:00+03:00`. В этом случае вам нужно указать значение `2021-01-01T00:00:00+03:00` в поле Начальное значение идентификатора, а в SQL-запросе произвести преобразование с помощью функции `to_timestamp_tz`, например:

    ```
    select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-
    DD"T"HH24:MI:SSTZH:TZM')
    ```

    Подробнее о функциях `to_timestamp` и `to_timestamp_tz` см. в официальной документации Oracle.

  > Для обращения к Oracle DB вам нужно установить пакет Astra Linux libaio1.

- Firebird® SQL.

  Например:

  ```
  firebirdsql://{user}:{password}@{server}:{port}/{database}
  ```

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

Если возникает проблема подключения к firebird на Windows, используйте полный путь до файла с базой данных, например:

```
firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB
```

- ClickHouse.

  Например:

  ```
  clickhouse://{user}:{password}@{server}:{port}/{database}
  ```

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

  KUMA поддерживает работу со следующими типами данных:

  - Данные, которые можно привести к строковому формату (например, строки, числовые значения и BLOB-объекты), отображаются в виде строк.
  - Массивы данных и карты отображаются в формате JSON или с помощью встроенного механизма `go fmt.Sprintf("%v",v)` показываются оптимальным доступным образом.

  Подключение к ClickHouse может осуществляться двумя способами:

  - Без использования учетных данных: необходимо ввести URL-адрес `clickhouse://host:port/database`.
  - С учетными данными: требуется использовать URL-адрес `clickhouse://user:password@host:port/database`.

  При использовании шифрования TLS по умолчанию коннектор работает только по порту 9440. Если шифрование TLS не используется, по умолчанию коннектор работает с ClickHouse только по порту 9000.

  > Коннектор не работает по протоколу http.

  Если на сервере с ClickHouse настроен режим шифрования TLS, а в параметрах коннектора в раскрывающемся списке **Режим TLS** выбрано **Выключено** или наоборот, соединение с базой данных не будет установлено.

  > **Режим TLS** используется только если указан драйвер ClickHouse.

  Если вы хотите подключиться к ClickHouse KUMA, вам нужно в параметрах коннектора с типом **SQL** указать тип секрета **PublicPKI**, который содержит закрытый ключ PEM, закодированный в base64, и открытый ключ.

  В параметрах коннектора с типом **SQL** для типа соединения ClickHouse вам нужно выбрать **Выключено** в раскрывающемся списке **Режим TLS**. Это значение недопустимо указывать, если для аутентификации используется сертификат. Если в раскрывающемся списке **Режим TLS** вы выбираете **Нестандартный CA**, в поле **Секрет** вам нужно указать ID секрета типа certificate. Вам также нужно выбрать одно из следующих значений в раскрывающемся списке **Тип авторизации**:

  - **Выключено**. При выборе этого значения вам нужно оставить пустым значение в поле **Секрет**.
  - **Обычная**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Секрет** указан ID секрета типа credentials.
  - **PublicPKI**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Секрет** указан ID секрета типа PublicPKI.

Если в начальном значении идентификатора есть указание времени (`datetime`), в запросе необходимо ввести переменную для преобразования времени (`parseDateTimeBestEffort`). Например, если время указано как `2021-01-01 00:10:00`, то запрос будет следующим:

```
select connections, username, host, login_time  from connections where login_time >
parseDateTimeBestEffort(?) order by login_time
```

В SQL-запросах поддерживается последовательный запрос сведений из базы данных. Например, если в поле **Запрос** указать SQL-запрос `select * from <название таблицы с данными> where id > <плейсхолдер>`, при первом обращении к таблице в качестве значения плейсхолдера будет использоваться значение поля **Начальное значение идентификатора**. При этом в сервисе, в котором используется SQL-коннектор, сохраняется идентификатор последней прочитанной записи, и во время следующего обращения к базе данных в качестве значения плейсхолдера в запросе будет использоваться идентификатор этой записи.

> В строку запроса рекомендуется добавлять команду `order by`, после которой указывается поле для сортировки. Например, `select * from table_name where id > ? order by id`.

Примеры SQL-запросов

SQLite, Firebird, MySQL, MariaDB, ClickHouse – `select * from table_name where id > ? order by id`

MsSQL – `select * from table_name where id > @p1 order by id`

PostgreSQL, Cockroach – `select * from table_name where id > $1 order by id`

Oracle – `select * from table_name where id > :val order by id`

Коннектор, тип file

Коннекторы с типом **file** используются для получения данных из текстовых файлов при работе с агентами Windows и Linux. Одна строка текстового файла считается одним событием. В качестве разделителя строк используется `\n`.

Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом **file**, 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.

Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.

Для чтения Windows-файлов вам нужно создать коннектор с типом **file** и установить агент на Windows вручную. Windows-агент не должен читать свои файлы в папке, где установлен агент. Коннектор будет работать, даже если файловая система FAT: если дефрагментировать диск, коннектор перечитает все файлы с начала, так все inode файлов сбрасываются.

> Мы не рекомендуем запускать агент под учетной записью администратора; необходимо, чтобы права чтения на папки/файлы были настроены для учетной записи агента. Мы не рекомендуем ставить агент на важные системы, лучше пересылать журналы и читать их на отдельных хостах с агентом.

Для каждого файла, с которым взаимодействует коннектор с типом **file**, создается файл состояния (states.ini) с параметрами `offset`, `dev`, `inode` и `filename`. Файл состояния позволяет коннектору при перечитывании файла возобновлять чтение с места, где коннектор остановился в последний раз, а не начинать чтение заново. Существуют следующие особенности перечитывания файлов:

- Если параметр `inode` в файле состояния изменится, при перечитывании файла, которому соответствует файл состояния, коннектор начнет чтение заново. При удалении и повторном создании файла параметр `inode` в соответствующем файле состояния может не измениться. В этом случае при перечитывании файла коннектор возобновит чтение на основании параметра `offset`.
- Если файл был обрезан или уменьшился его размер, при перечитывании файла коннектор начнет чтение заново.
- Если файл был переименован, при перечитывании файла коннектор возобновит чтение с места, где коннектор остановился в последний раз.
- Если директория с файлом была перемонтирована, при перечитывании файла коннектор возобновит чтение с места, где коннектор остановился в последний раз. Вы можете указать путь к файлам, с которыми взаимодействует коннектор, при настройке коннектора в поле **Путь к файлу**.

Доступные параметры коннектора с типом **file** 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.
Тип	Тип коннектора – **file**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание

Путь к файлу	Коннекторы с типом **file** используются для получения данных из текстовых файлов при работе с агентами Windows и Linux. Одна текстового файла считается одним событием. В качестве разделителя строк используется `\n`.
	
	Полный путь к файлу, с которым коннектор выполняет взаимодействие. Поддерживаются форматы путей как для Linux, так и для например:
	• для Windows: `C:\var\log\test123.log`
	• для Linux: `/var/log/test123.log`
	Недопустимо указывать пути, соответствующие следующим регулярным выражениям:
	• `(?i)^[a-zA-Z]:\\Program Files`
	• `(?i)^[a-zA-Z]:\\Program Files\(x86\)`
	• `(?i)^[a-zA-Z]:\\Windows`
	• `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA`
	В приведенных регулярных выражениях двойные обратные косые черты (\\) используются системой в качестве части синтаксис регулярного выражения для проверки пути и не должны указываться в самом пути вручную.
	Шаблоны масок для файлов и директорий
	
	Маски:
	• `'*'` – соответствует любой последовательности символов;
	• `'[' [ '^' ] { < диапазон символов > } ']'` – класс символов (не должен быть пустым);
	• `'?'` – соответствует любому одиночному символу.
	
	Диапазоны символов:
	• `[0-9]` – числа;
	• `[a-zA-Z]` – буквы латинского алфавита.
	Пример:
	Маски можно использовать как в путях Linux, так и Windows с заменой прямой косой черты на обратную:
	• Для Linux:
	  • `/var/log/*som?[1-9].log`
	  • `/mnt/dns_logs/*/dns.log`
	  • `/mnt/proxy/access*.log`
	• Для Windows:
	  • `C:\var\log\test123.log`
	  • `D:\data\*\report?.txt`
	
	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/*`

Параметр	Описание

	• `/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 л 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/`
	
	Ограничение количества отслеживаемых файлов по маске
	
	Количество одновременно отслеживаемых файлов по маске может быть ограничено параметром Ядра `max_user_watches`. Для просмотра з параметра выполните команду:
	
	`cat /proc/sys/fs/inotify/max_user_watches`
	
	Если количество файлов для отслеживания превышает значение параметра `max_user_watches`, коллектор больше не сможет считывать соб файлов и в журнале коллектора появится следующая ошибка:
	
	`Failed to add files for watching {"error": "no space left on device"}`
	
	Для продолжения правильной работы коллектора вы можете настроить правильную ротацию файлов, чтобы количество файлов не превышал параметра `max_user_watches`, или увеличить значение `max_user_watches`.
	
	Для увеличения значения параметра выполните команду:
	
	`sysctl fs.inotify.max_user_watches=< количество файлов >`
	
	`sysctl -p`
	
	Вы можете добавить значение параметра `max_user_watches` в sysctl.conf, чтобы значение сохранялось всегда.
	
	После того, как вы увеличите значение параметра `max_user_watches`, коллектор успешно продолжит работу.
	
	Обязательный параметр.

Время ожидания изменений, сек	Время в секундах, в течение которого файл не должен обновляться, чтобы KUMA выполнила с ним действие, указанное в раскры списке **Действие после таймаута**. Значение по умолчанию: `0` – если файл не обновляется, KUMA не выполняет с ним никакого , Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Дополнительные параметры** в поле **Интер запросов, мс**.
Действие после таймаута	Действие, которое KUMA выполняет с файлом по прошествии времени, указанного в поле **Время ожидания изменений, сек**: • **Ничего не делать**. Значение по умолчанию. • **Добавление суффикса** – добавить к названию файла расширение .kuma_processed и не обрабатывать файл даже при его с • **Удаление** – удалить файл.

Параметр	Описание
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно со auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для мех auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся спи **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. KUMA классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие записи `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty= old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a0 a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет испо префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например, обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F78` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.52 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid=1 pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses= comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:12061` поскольку они не передают важной для событий информации.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.

Параметр	Описание
Интервал запросов, мс	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории. Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Основные параметры** в поле **Время ожидания изменений, сек**. Мы рекомендуем ввести значение меньше, чем значение, которое вы ввели в поле **TTL буфера событий**, так как это может негативно сказаться на работе функции Auditd.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор KUMA и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 700 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором KUMA. Вы можете просмотреть в метриках KUMA, сколько оперативной памяти сервера использует коллектор KUMA. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором KUMA.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.

Коннектор, тип 1c-log

Коннекторы с типом **1c-log** используются для получения данных из технологических журналов программы 1С при работе с агентами Linux. В качестве разделителя строк используется `\n`. Из многострочной записи о событии коннектор принимает только первую строку.

Доступные параметры коннектора с типом **1c-log** 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.
Тип	Тип коннектора – **1c-log**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный параметр.
Путь к директории	Полный путь к директории с файлами, с которыми требуется выполнять взаимодействие, например `/var/log/1c/logs/`. **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/` Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.
Интервал запросов, мс.	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории.
Кодировка символов	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.

Схема работы коннектора:

1. Происходит поиск всех файлов технологических журналов 1С. Требования к файлам журналов:

   - Файлы с расширением LOG создаются в директории журналов (по умолчанию `/var/log/1c/logs/`) в поддиректории каждого процесса (см. рисунок по ссылке ниже).

Пример поддерживаемой структуры технологических журналов 1с

```
/var/log/1c
└── logs
    ├── ragent_1426
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── ragent_1427
    │   ├── 22121518.log
    │   ├── 22121519.log
    │   ├── 22121520.log
    │   ├── 22121521.log
    │   ├── 22121522.log
    │   ├── 22121523.log
    │   ├── 22121600.log
    │   ├── 22121601.log
    │   ├── 22121602.log
    │   ├── 22121603.log
    │   ├── 22121604.log
    │   └── 22121605.log
    ├── rmngr_1542
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── rmngr_1544
    │   ├── 22121518.log
    │   ├── 22121519.log
```

Пример поддерживаемой структуры технологических журналов 1с

- События записываются в файл в течение часа, после чего создается следующий файл журнала.
- Название файлов имеет следующий формат: <ГГ><ММ><ДД><ЧЧ>.log. Например, 22111418.log – файл, созданный в 2022 году, в 11 месяце, 14 числа в 18 часов.
- Каждое событие начинается с времени события в формате <мм>:<сс>.<микросекунды>-<длительность в микросекундах>.

2. Отбрасываются уже обработанные файлы. Сведения об обработанных файлах хранятся в файле /<рабочая директория коллектора>/1c_log_connector/state.json.
3. Принимаются на обработку новые события, при этом время события приводится к формату RFC3339.
4. Обрабатывается следующий в очереди файл.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-log на ОС Windows не поддерживается. Для обеспечения передачи файлов с журналами 1С для обработки коллектором KUMA выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.

  2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).

  3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Из многострочной записи о событии на обработку принимается только первая строка.

- Нормализатор обрабатывает только следующие типы событий:

  - ADMIN.
  - ATTN.
  - CALL.
  - CLSTR.
  - CONN.
  - DBMSSQL.
  - DBMSSQLCONN.
  - DBV8DBENG.
  - EXCP.
  - EXCPCNTX.
  - HASP.
  - LEAKS.
  - LIC.
  - MEM.
  - PROC.
  - SCALL.
  - SCOM.
  - SDBL.
  - SESN.

- SINTEG.
- SRVC.
- TLOCK.
- TTIMEOUT.
- VRSREQUEST.
- VRSRESPONSE.

Коннектор, тип 1c-xml

Коннекторы с типом **1c-xml** используются для получения данных из журналов регистрации программы 1С при работе с агентами Linux. При обработке коннектором многострочные события преобразовываются в однострочные.

Доступные параметры коннектора с типом **1c-xml** 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.
Тип	Тип коннектора – **1c-xml**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
Путь к директории	Полный путь к директории с файлами, с которыми требуется выполнять взаимодействие, например `/var/log/1c/logs/`. **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/` Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.
Интервал запросов, мс	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Схема работы коннектора:

1. Происходит поиск всех файлов с журналами 1С с расширением XML внутри указанной директории. Журналы помещаются в директорию или вручную, или через приложение, написанное на языке 1С, например с помощью функции `ВыгрузитьЖурналРегистрации()`. Коннектор поддерживает журналы, полученные только таким образом. Подробнее о том, как получить журналы 1С, см. в официальной документации 1С.

2. Файлы сортируются по возрастанию времени последнего изменения. Коннектор сохраняет сведения о последнем обработанном файле и не обрабатывает файлы, измененные раньше него. При сбросе состояния (например, при обнаружении пустого файла) ранее обработанные файлы могут быть обработаны повторно..

   Сведения об обработанных файлах хранятся в файле /<рабочая директория коллектора>/1c_xml_connector/state.ini и имеют следующий формат: `offset=< число >\ndev= < число >\ninode=< число >`.

3. В каждом непрочитанном файле определяются события.

4. События из файла по очереди принимаются на обработку, при этом многострочные события преобразовываются в однострочные события.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-xml на ОС Windows не поддерживается. Для обеспечения передачи файлов с журналами 1С для обработки коллектором KUMA выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.

  2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).

  3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Не читаются файлы с неправильным форматом событий. Например, если теги события в файле на русском языке, коллектор не прочитает такие события.

Пример правильного XML-файла с событием.

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns: v8e="http://v8.1c.ru/eventLog"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <v8e:Event>
    <v8e:Level>Information</v8e:Level>
    <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
    <v8eApplicationName>generator.go</v8e:ApplicationName>
<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
    <v8e:Event>Test event type: Count test</v8e:Event>
    <v8e:EventPresentation></v8e:Event Presentation>
    <v8e:User>abcd_1234</v8e:User>
    <v8e:UserName>TestUser</v8e:UserName>
    <v8e:Computer>Test OC</v8e:Computer>
    <v8e:Metadata></v8e:Metadata>
    <v8e:MetadataPresentation></v8e:MetadataPresentation>
    <v8e:Comment></v8e:Comment>
    <v8e:Data>
      <v8e:Name></v8e:Name>
      <v8e:CurrentOSUser></v8e:CurrentOSUser>
    </v8e:Data>
    <v8e:DataPresentation></v8e:DataPresentation>
    <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
    <v8e:TransactionID></v8e:TransactionID>
    <v8e:Connection>0</v8e:Connection>
    <v8e:Session></v8e:Session>
    <v8e:ServerName>kuma-test</v8e:ServerName>
    <v8e:Port>80</v8e:Port>
    <v8e:SyncPort>0</v8e:SyncPort>
  </v8e:Event>
</v8e:EventLog>
```

Пример обработанного события.

```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```

Пример обработанного события

- При наличии в директории пустого файла журнала (файла без событий) коннектор сбрасывает сведения о последнем обработанном файле. В результате ранее обработанные файлы могут быть обработаны повторно. Чтобы избежать повторной обработки событий, используйте один из следующих способов:
  - Используйте маску имени файла, исключающую новые пустые файлы из обработки, и переименуйте файл после записи первого события.
  - Перед созданием нового файла переименуйте уже обработанные файлы так, чтобы они перестали соответствовать маске поиска коннектора.
- Если дополнить уже прочитанный коннектором файл новыми событиями и если этот файл не является последним прочитанным файлом в директории, все события из файла будут обработаны заново.

Коннектор, тип diode

Коннекторы с типом **diode** используются для однонаправленной передачи данных в промышленных ICS-сетях с помощью диода данных. Доступные параметры коннектора с типом **diode** 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.
Тип	Тип коннектора – **diode**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
Директория с событиями от диода данных	Полный путь к директории на сервере коллектора KUMA, в которую диод данных перемещает файлы с событиями из изолированного сегмента сети. После считывания коннектором файлы удаляются из директории. Максимальная длина пути: до 255 символов в кодировке Unicode. **Ограничения при использовании префиксов к путям** 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/` Обязательный параметр.

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. Вам нужно выбрать одинаковое значение в раскрывающемся списке **Разделитель** в параметрах коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Интервал запросов, сек.	Интервал в секундах для считывания файлов из директории с событиями от диода данных. Значение по умолчанию: 2 секунды.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**. Вам нужно выбрать одинаковое значение в раскрывающемся списке **Snappy** в параметрах коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

Коннектор, тип ftp

Коннекторы с типом **ftp** используются для получения данных по протоколу File Transfer Protocol при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **ftp** 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.
Тип	Тип коннектора – **ftp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
URL	URL-адрес файла или маски файлов, начинающийся со схемы `'ftp://'`. Для маски файлов вы можете использовать символы `* ? [...]`. **Шаблоны масок для файлов** Маски: • `'*'` – соответствует любой последовательности символов; • `'[' [ '^' ] { < диапазон символов > } ']'` – класс символов (не должен быть пустым); • `'?'` – соответствует любому одиночному символу. Диапазоны символов: • `[0-9]` – числа; • `[a-zA-Z]` – буквы латинского алфавита. Пример: Маски можно использовать как в путях Linux, так и Windows с заменой прямой косой черты на обратную: • Для Linux: • `/var/log/*som?[1-9].log` • `/mnt/dns_logs/*/dns.log` • `/mnt/proxy/access*.log` • Для Windows: • `C:\var\log\test123.log` • `D:\data\*\report?.txt` Если URL-адрес не содержит номер порта FTP-сервера, автоматически указывается номер порта `21`. Обязательный параметр.
Секрет	
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип nfs

Коннекторы с типом **nfs** используются для получения данных по протоколу Network File System при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **nfs** 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.
Тип	Тип коннектора – **nfs**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	Путь до удаленной директории в формате `nfs://< имя хоста >/< путь >`. Обязательный параметр.
Маска имени файла	Маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`".
Интервал запросов, сек.	Интервал опроса в секундах. Промежуток времени, через который перечитываются файлы с удаленной системы. Значение по умолчанию: `0`.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип wmi

Коннекторы с типом **wmi** используются для получения данных с помощью Windows Management Instrumentation при работе с агентами Windows. Доступные параметры коннектора с типом **wmi** 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.
Тип	Тип коннектора – **wmi**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес коллектора, который вы создали для получения данных с помощью Windows Management Instrumentation, например `kuma-collector.example.com:7221`. При создании коллектора автоматически создается агент, который будет получать данные на удаленном устройстве и перенаправлять их в сервис коллектора. Если вы знаете, на каком сервере будет установлен сервис коллектора, URL-адрес известен заранее. Вы можете ввести URL-адрес коллектора в поле **URL** после завершения мастера установки. Для этого вам нужно предварительно скопировать URL-адрес коллектора в разделе **Ресурсы** → **Активные сервисы**. Обязательный параметр.
Учетные данные по умолчанию	Вам нужно указать учетные данные для подключения к хостам, которые можно использовать по умолчанию в таблице **Удаленные хосты**. Поле является обязательным, если в таблице **Удаленные хосты** не указан секрет хотя бы для одного хоста.

Параметр	Описание
Удаленные хосты	Параметры удаленных Windows-устройств, к которым требуется установить подключение: • **Сервер** – IP-адрес или имя устройства, с которого необходимо принимать данные, например `machine-1`. Не допускается использование символов кириллицы. Обязательный параметр. • **Домен** – название домена, в котором расположено удаленное устройство, например, `example.com`. Не допускается использование символов кириллицы. Обязательный параметр. • **Тип журналов** – название журналов Windows, которые требуется получить. По умолчанию в этом раскрывающемся списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами. Для этого введите название пользовательских журналов в поле **Журналы Windows**, после чего нажмите на клавишу **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов. Журналы, доступные по умолчанию: • Application. • ForwardedEvents. • Security. • System. • HardwareEvents. Если в одном из подключений WMI используется хотя бы один журнал с неверным названием, агент, использующий коннектор, не будет получать события из всех журналов данного подключения, даже если названия остальных журналов указаны верно. При этом подключения WMI-агента, в которых все названия журналов указаны правильно, будет работать правильно. Обязательный параметр. • **Секрет** – учетные данные для доступа к удаленному Windows-устройству с правами на чтение журналов. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите **Создать**. При создании секрета в поле **Пользователь** не требуется указывать домен для доступа к хосту, поскольку используется значение, указанное в поле **Домен** в таблице **Удаленные хосты**. Если вы хотите изменить параметры существующего секрета, нажмите на значок карандаша ✎. Если оставить в этом поле значение **по умолчанию**, для подключения к удаленным Windows-устройствам будут использоваться учетные данные, указанные в поле **Учетные данные, используемые по умолчанию**. **Как создать 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**. Вы можете добавить несколько удаленных Windows-устройств или удалить удаленное Windows-устройство. Для добавления удаленного Windows-устройства нажмите на кнопку **+ Добавить**. Для удаления удаленного Windows-устройства установите рядом с ним флажок и нажмите на кнопку **Удалить**. Также с помощью кнопки **Импортировать** вы можете импортировать файл со списком удаленных Windows-устройств в формате TSV, чтобы не заполнять поля вручную, когда таких устройств много. KUMA автоматически подставит данные из файла и выполнит проверку. Для некорректно заполненных полей отобразится ошибка. Вы можете внести правки для таких полей вручную и сохранить параметры.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание
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.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Получение событий с удаленного устройства

Условия для получения событий с удаленного устройства Windows с агентом KUMA:

- Для запуска агента KUMA на удаленном устройстве вам нужно использовать учетную запись с правами Log on as a service.
- Для получения событий от агента KUMA вам нужно использовать учетную запись с правами Event Log Readers. Для серверов домена может быть создана одна такая учетная запись, чтобы через групповую политику ее права на чтение логов можно было распространить на все серверы и рабочие станции домена.
- На удаленных устройствах Windows необходимо открыть следующие TCP-порты 135, 445, 49152-65535.
- На удаленных устройствах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

Коннектор, тип wec

Коннекторы с типом **wec** используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС хоста под управлением Windows при работе с агентами Windows. Доступные параметры коннектора с типом **wec** 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.
Тип	Тип коннектора – **wec**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес коллектора, который вы создали для получения данных с помощью Windows Event Collector, например `kuma-collector.example.com:7221`. При создании коллектора автоматически создается агент, который будет получать данные на удаленном устройстве и перенаправлять их в сервис коллектора. Если вы знаете, на каком сервере будет установлен сервис коллектора, URL-адрес известен заранее. Вы можете ввести URL-адрес коллектора в поле **URL** после завершения мастера установки. Для этого вам нужно предварительно скопировать URL-адрес коллектора в разделе **Ресурсы** → **Активные сервисы**. Обязательный параметр.
Журналы Windows	Названия журналов Windows, которые требуется получить. По умолчанию в этом раскрывающемся списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами. Для этого введите название пользовательских журналов в поле **Журналы Windows**, после чего нажмите на клавишу **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов. Преднастроенные журналы: • Application. • ForwardedEvents. • Security. • System. • HardwareEvents. Если неверно указать название хотя бы одного журнала, в этом случае агент, использующий коннектор, не будет получать события из всех журналов, даже если названия остальных журналов указаны верно. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
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.
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Для запуска агента KUMA на удаленном устройстве вам нужно использовать сервисную учетную запись с правами Log on as a service. Для получения событий из журнала ОС сервисная учетная запись также должна обладать правами Event Log Readers.

Вы можете создать одну учетную запись с правами Log on as a service и Event Log Readers, а затем права этой учетной записи на чтение журналов распространить на все серверы и рабочие станции домена с помощью групповой политики.

Мы рекомендуем запретить для сервисной учетной записи возможность интерактивного входа.

Коннектор, тип etw

Коннекторы с типом **etw** используются для получения расширенных журналов DNS-серверов. Доступные параметры коннектора с типом **etw** 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.
Тип	Тип коннектора – **etw**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес DNS-сервера. Обязательный параметр.
Имя сессии	Имя сессии, которое соответствует ETW-провайдеру Microsoft-Windows-DNSServer {EB79061A-A566-4698-9119-3ED2807060E7}. Если в коннекторе с типом **etw** имя сессии указано неправильно, указан неправильный провайдер в сессии или указан неправильный режим отправки событий (для правильной отправки событий на стороне Windows Server должен быть указан режим Real time или File and Real time), от агента не будут поступать события, в журнале агента на Windows будет зарегистрирована ошибка, а статус агента будет зеленым. При этом попытки получить события каждые 60 сек не будет. Если вы изменяете параметры сессии на стороне Windows, вам нужно перезапустить агент etw и/или сессию, чтобы изменения были применены. Подробнее о настройке параметров сессии на стороне Windows для получения событий DNS-сервера, см. в разделе Настройка получения событий DNS-сервера с помощью агента ETW. Обязательный параметр.
Извлекать информацию о событии	Переключатель, включающий извлечение минимального количества данных о событии, которое возможно без необходимости скачивать сторонние метаданные с диска. Такой способ позволяет сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и извлекаются все данные о событии.
Извлекать свойства события	Переключатель, включающий извлечение свойств событий. Если этот переключатель выключен, свойства события не будут извлечены и это позволит сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и свойства события извлекаются. Вы можете включить переключатель **Извлекать свойства события**, только если включен переключатель **Извлекать информацию о событии**.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
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.

Параметр	Описание
Сжатие	Раскрывающийся список, позволяющий настроить использование сжатия Snappy: • **Выключено**. Это значение выбрано по умолчанию. • **С помощью Snappy**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Коннектор, тип snmp

Коннекторы с типом **snmp** используются для получения данных с помощью Simple Network Management Protocol при работе с агентами Windows и Linux. Для обработки событий, полученных по протоколу SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:

- snmpV1.
- snmpV2.
- snmpV3.

В агенте можно использовать только один коннектор **snmp**, созданный в параметрах агента. При необходимости использования нескольких коннекторов **snmp**, один или все коннекторы **snmp** нужно создать как отдельный ресурс и выбрать в параметрах подключения.

Доступные параметры коннектора с типом **snmp** 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.
Тип	Тип коннектора – **snmp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Параметр	Описание

SNMP-ресурс	Параметры подключения к SNMP-ресурсу:
	• **Версия SNMP** – версия используемого протокола SNMP.
	Обязательный параметр.
	• **Хост** – имя или IP-адрес хоста. Доступные форматы:
	  • `<имя хоста>`;
	  • `<IPv4-адрес>`;
	  • `<IPv6-адрес>`.
	Обязательный параметр.
	• **Порт** – Номер порта для подключения к хосту. Как правило используется значение `161` или `162`.
	Обязательный параметр.
	• **Секрет** – секрет, в котором хранятся учетные данные для подключения через Simple Network Management Protocol. Тип секрета должен соответствовать версии SNMP.
	Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать 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**.
	Обязательный параметр.
	Вы можете добавить несколько подключений к SNMP-ресурсам или удалить подключение к SNMP-ресурсу. Для добавления подключения к SNMP-ресурсу нажмите на кнопку **+ SNMP-ресурс**. Для удаления подключения к SNMP-ресурсу нажмите рядом с ним на значок удаления ✕.

Параметры	Правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные параметры: • **Название параметра** – название для типа данных, например `Имя узла` или `Время работы узла`. Обязательный параметр. • **OID** – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий, например `1.3.6.1.2.1.1.5`. KUMA запрашивает данные с помощью команды SNMP GET. Обязательный параметр. • **Ключ** – уникальный идентификатор, который возвращается в ответ на запрос к устройству со значением запрошенного параметра, например `sysName`. Вы можете обращаться к ключу при нормализации данных. Обязательный параметр. • **MAC-адрес** – если этот флажок установлен, KUMA правильно производит декодирование данных, где OID содержит данные о MAC-адресе в формате OctetString. После декодирования MAC-адрес будет преобразован в формат `Строка` вида XX:XX:XX:XX:XX:XX. Вы можете выполнить следующие действия с правилами: • Добавить несколько правил. Для добавления правила нажмите на кнопку **+ Добавить**. • Удалить правила. Для удаления правила установите рядом с ним флажок и нажмите на кнопку **Удалить**. • Очистить параметры правил. Для этого нажмите на кнопку **Очистить значения**.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип snmp-trap

Коннекторы с типом **snmp-trap** используются для пассивного приема событий с помощью ловушек SNMP (англ. SNMP traps) при работе с агентами Windows и Linux. В коннекторе события snmp-trap принимаются и подготавливаются к нормализации путем сопоставления идентификаторов SNMP-объектов с временными ключами. Затем сообщение необходимо передать в JSON-нормализатор, где временные ключи будут сопоставлены с полями KUMA и будет создано событие. Для обработки событий, полученных по SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:

- snmpV1.
- snmpV2.

Доступные параметры коннектора с типом **snmp-trap** 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.
Тип	Тип коннектора – **snmp-trap**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

SNMP-ресурс	Параметры соединения для получения событий snmp-trap:
	• **Версия SNMP** – версия используемого протокола SNMP:
	  • **snmpV1**;
	  • **snmpV2**.
	  Например, Windows по умолчанию использует версию протокола SNMP snmpV2.
	  Обязательный параметр.
	• **URL** – URL-адрес для получения событий SNMP trap. Вы можете ввести URL-адрес в одном из следующих форматов:
	  • `< имя хоста >:< номер порта >`;
	  • `< IPv4-адрес >:< номер порта >`;
	  • `< IPv6-адрес >:< номер порта >`;
	  • `:< номер порта >`.
	  Обязательный параметр.
	Вы можете добавить несколько соединений или удалить соединение. Для добавления соединения нажмите на кнопку **+ SNMP-ресурс**. Для удаления SNMP-ресурса нажмите рядом с ним на значок удаления ✕.

Параметр	Описание
Параметры	Правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные параметры: • **Название параметра** – название для типа данных, например `Имя узла` или `Время работы узла`. Обязательный параметр. • **OID** – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий, например `1.3.6.1.2.1.1.5`. KUMA запрашивает данные с помощью команды SNMP GET. Обязательный параметр. • **Ключ** – уникальный идентификатор, который возвращается в ответ на запрос к устройству со значением запрошенного параметра, например `sysName`. Вы можете обращаться к ключу при нормализации данных. Обязательный параметр. • **MAC-адрес** – если этот флажок установлен, KUMA правильно производит декодирование данных, где OID содержит данные о MAC-адресе в формате OctetString. После декодирования MAC-адрес будет преобразован в формат `Строка` вида XX:XX:XX:XX:XX:XX. Вы можете выполнить следующие действия с правилами: • Добавить несколько правил. Для добавления правила нажмите на кнопку **+ Добавить**. • Удалить правила. Для удаления правила установите рядом с ним флажок и нажмите на кнопку **Удалить**. • Очистить параметры правил. Для этого нажмите на кнопку **Очистить значения**. • Заполнить таблицу сопоставлениями для значений OID, поступающих в журналах WinEventLog. Для этого нажмите на кнопку **Применить значения OID для WinEventLog**. Если в поступающих событиях необходимо определить и нормализовать больше данных, дополните таблицу строками с перечнем OID-объектов и их ключей. Данные обрабатываются по принципу списка разрешенных: объекты, которые не указаны в таблице, не будут переданы в нормализатор для дальнейшей обработки.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**. При получении событий snmp-trap из Windows с русской локализацией мы рекомендуем изменить кодировку символов в коннекторе с типом **snmp-trap** на Windows 1251, если в событии получены недопустимые символы.

Настройка источника SNMP-trap сообщений для Windows

Настройка устройства Windows для отправки SNMP-trap сообщений в коллектор KUMA происходит в несколько этапов:

1. **Настройка и запуск служб SNMP и SNMP Trap**
2. **Настройка службы Event to Trap Translator**

События от источника SNMP-trap сообщений должен принимать коллектор KUMA, в котором используется коннектор типа snmp-trap и нормализатор типа json.

Настройка и запуск служб SNMP и SNMP Trap

Чтобы настроить и запустить службы SNMP и SNMP Trap в Windows 10:

1. Откройте раздел **Settings** → **Apps** → **Apps and features** → **Optional features** → **Add feature** → **Simple Network Management Protocol (SNMP)** и нажмите **Install**.
2. Дождитесь завершения установки и перезагрузите компьютер.
3. Убедитесь, что служба SNMP запущена. Если какие-то из перечисленных ниже служб не запущены, включите их:
   - **Services** → **SNMP Service**.
   - **Services** → **SNMP Trap**.

4. Нажмите правой кнопкой мыши на службе **Services** → **SNMP Service**, в контекстном меню выберите **Properties** и задайте следующие параметры:

   - На вкладке **Log On** установите флажок **Local System account**.

   - На вкладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).

   - На вкладке **Traps**:

     - В поле **Community Name** введите **community public** и нажмите **Add to list**.

     - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или хост сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.

   - На вкладке **Security**:

     - Установите флажок **Send authentication trap**.

     - В таблице **Accepted community names** нажмите **Add**, а затем введите **Community Name public**, указав в качестве **Community rights** значение **READ WRITE**.

     - Установите флажок **Accept SNMP packets from any hosts**.

5. Нажмите **Apply** и подтвердите выбор.

6. Нажмите правой кнопкой мыши на службу **Services** → **SNMP Service** и выберите **Restart**.

Чтобы настроить и запустить службы SNMP и SNMP Trap в Windows XP:

1. Откройте раздел **Start** → **Control Panel** → **Add or Remove Programs** → **Add/Remove Windows Components** → **Management and Monitoring Tools** → **Details**.

2. Выберите **Simple Network Management Protocol** и **WMI SNMP Provider**, затем нажмите **OK** → **Next**.

3. Дождитесь завершения установки и перезагрузите компьютер.

4. Убедитесь, что служба SNMP запущена. Если какие-то из перечисленных ниже служб не запущены, включите их, выбрав для параметра **Startup type** значение **Automatic**:

   - **Services** → **SNMP Service**.

   - **Services** → **SNMP Trap**.

5. Нажмите правой кнопкой мыши на службе **Services** → **SNMP Service**, в контекстном меню выберите **Properties** и задайте следующие параметры:

   - На вкладке **Log On** установите флажок **Local System account**.

   - На вкладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).

- На вкладке **Traps**:
  - В поле **Community Name** введите **community public** и нажмите **Add to list**.
  - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или хост сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.
- На вкладке **Security**:
  - Установите флажок **Send authentication trap**.
  - В таблице **Accepted community names** нажмите **Add**, а затем введите **Community Name public**, указав в качестве **Community rights** значение **READ WRITE**.
  - Установите флажок **Accept SNMP packets from any hosts**.

6. Нажмите **Apply** и подтвердите выбор.
7. Нажмите правой кнопкой мыши на службу **Services** → **SNMP Service** и выберите **Restart**.

Изменение порта службы snmptrap

При необходимости вы можете изменить порт службы snmptrap.

Чтобы изменить порт службы snmptrap:

1. Откройте папку C:\Windows\System32\drivers\etc.
2. Откройте файл **services** с помощью программы Notepad от имени администратора.
3. В разделе файла **service name** для службы **snmptrap** укажите порт коннектора snmp-trap, добавленный в коллектор KUMA.
4. Сохраните файл.
5. Откройте панель управления и выберите **Administrative Tools** → **Services**.
6. Нажмите на службу **SNMP Service** правой кнопкой мыши и выберите **Restart**.

Настройка службы Event to Trap Translator

Чтобы настроить службу Event to Trap Translator, с помощью которой события Windows переводятся в SNMP-trap сообщения:

1. Наберите в командной строке `evntwin` и нажмите **Enter**.
2. В переключателе **Configuration type** выберите **Custom**, а затем нажмите на кнопку **Edit**.
3. В блоке параметров **Event sources** найдите и добавьте с помощью кнопки **Add** события, которые вы хотите отправить в коллектор KUMA с установленным коннектором SNMP Trap.
4. Нажмите на кнопку **Settings**, в открывшемся окне установите флажок **Don't apply throttle** и нажмите **OK**.
5. Нажмите **Apply** и подтвердите выбор.

Коннектор, тип kata/edr

Коннекторы с типом **kata/edr** используются для получения данных KEDR по API. Доступные параметры коннектора с типом **kata/edr** 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.
Тип	Тип коннектора – **kata/edr**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный 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.
Секрет	Секрет, в котором хранятся учетные данные для подключения к серверу KATA/EDR. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. Обязательный параметр.
Внешний ID	Идентификатор для внешних систем. KUMA автоматически генерирует идентификатор и указывает его в этом поле.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. Мы рекомендуем применять конвертацию, только если в полях нормализованного события отображаются недопустимые символы. По умолчанию значение не выбрано.

Параметр	Описание
Максимальное количество событий	Максимальное количество событий в одном запросе. По умолчанию используется значение, указанное на сервере KATA/EDR.
Время ожидания получения событий	Время ожидания получения событий от сервера KATA/EDR в секундах. Значение по умолчанию: `0` – используется значение, указанное на сервере KATA/EDR.
Время ожидания ответа	Время ожидания ответа от сервера KATA/EDR в секундах. Значение по умолчанию: `0` – 1800 секунд.
Фильтр KEDRQL	Фильтр запросов к серверу KATA/EDR. Подробнее о языке запросов см. в Справке KEDR.

Коннектор, тип vmware

Коннекторы с типом **vmware** используются для получения данных VMware vCenter по API. Доступные параметры коннектора с типом **vmware** 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.
Тип	Тип коннектора – **vmware**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес API VMware. Вам нужно указать имя хоста и номер порта в URL-адресе. Вы можете указать только один URL-адрес. Обязательный параметр.
Учетные данные VMware	Секрет, где хранится логин и пароль для подключения к API VMware. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать 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**. Обязательный параметр.
Время ожидания, сек	Время ожидания в секундах между запросом, который не вернул события, и новым запросом. Значение по умолчанию: 5 секунд. Если вы указываете `0`, используется значение по умолчанию.
Количество запрашиваемых событий	Количество запрашиваемых событий из API VMware за один запрос. Значение по умолчанию: `100`. Максимальное значение: `1000`.
Начальная временная метка	Дата и время, начиная с которого события будут считываться из API VMware. По умолчанию события считываются из API VMware с момента запуска коллектора. При запуске после остановки коллектора, считывание событий будет происходить с последней сохраненной даты.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

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.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Коннектор, тип elastic

Коннекторы с типом **elastic** используются для получения данных Elasticsearch. Поддерживается работа с Elasticsearch версии 7.0.0. Доступные параметры коннектора с типом **elastic** 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.

Параметр	Описание
Тип	Тип коннектора – **elastic**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Соединение	Параметры подключения к серверу Elasticsearch: • **URL** – URL-адрес сервера Elasticsearch. Вы можете добавить несколько URL-адресов или удалить URL-адрес. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр. • **Индекс** – имя индекса в Elasticsearch. Обязательный параметр. • **Запрос** – запрос в Elasticsearch. Мы рекомендуем указывать в запросе параметр `size` для предотвращения проблем с производительностью KUMA и Elasticsearch, а также параметр `sort` для направления сортировки. Для параметра `sort` в запросе возможны значения: `asc`, `desc` или пользовательское направление сортировки по конкретным полям в соответствии с синтаксисом Elasticsearch. Для сортировки по конкретному полю рекомендуется также указывать параметр `"missing" : "_first"` рядом с параметром `"order"` для предотвращения ошибок в случаях, когда это поле отсутствует в каком-либо документе. Например, `"sort": { "DestinationDnsDomain.keyword": {"order": "desc", "missing" : "_first" } }`. Подробнее о сортировке см. в документации Elasticsearch. Пример запроса: `"query" : { "match_all" : {} }, "size" : 25, "sort": {"_doc" : "asc"}` Обязательный параметр. • **Учетные данные Elastic** – секрет, в котором хранятся учетные данные для подключения к серверу Elasticsearch. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎. **Как создать 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**. • **Elastic fingerprint** – секрет, в котором хранятся секреты типа fingerprint для подключения к серверу Elasticsearch и секреты типа certificate для использования CA сертификата. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎. • **Интервал запросов, сек** – интервал выполнения между запросами к серверу Elasticsearch в секундах в случае, если в предыдущем запросе отсутствовали события. Если Elasticsearch содержал события в момент выполнения запроса, коннектор будет получать события до момента, пока не будут получены все доступные события из Elasticsearch. Вы можете добавить несколько подключений к серверу Elasticsearch или удалить подключение к серверу Elasticsearch. Для добавления подключения к серверу Elasticsearch нажмите на кнопку **+ Добавить подключение**. Для удаления подключения к серверу Elasticsearch нажмите рядом с ним на значок удаления ✕.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип office365

Коннекторы с типом **office365** используются для получения данных Microsoft 365 (Office 365) по API.

Доступные параметры коннектора с типом **office365** 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.
Тип	Тип коннектора – **office365**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Типы контента Office365	Типы контента, которые вы хотите получать в KUMA. Доступны следующие типы контента с информацией о действиях и событиях в Microsoft 365, сгруппированные в зависимости от источника информации: • **Audit.General**. • **Audit.AzureActiveDirectory**. • **Audit.Exchange**. • **Audit.Sharepoint**. • **DLP.All**. С подробной информацией о свойствах доступных типов контента и связанных с ними событиях можно ознакомиться на схеме на сайте Microsoft. Обязательный параметр. Можно выбрать один или несколько типов контента.
Идентификатор тенанта Office365	Уникальный идентификатор, получаемый после регистрации учетной записи в Microsoft 365. Если у вас его нет, обратитесь к вашему администратору или в Microsoft. Обязательный параметр.
ID клиента Office365	Уникальный идентификатор, получаемый после регистрации учетной записи в Microsoft 365. Если у вас его нет, обратитесь к вашему администратору или в Microsoft. Обязательный параметр.
Авторизация	Способ авторизации для подключения к Microsoft 365. Доступны следующие способы авторизации: • **PFX**. Использование секрета PFX. • **Токен**. Использование секрета token. Подробную информацию можно найти в разделе о секретах.
Учетные данные Office365	Поле становится доступно после выбора способа авторизации. Можно выбрать один из доступных секретов для авторизации или создать новый секрет выбранного типа. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Хост для аутентификации	URL, по которому будет выполняться подключение и авторизация. По умолчанию выполняется подключение по адресу https://login.microsoftonline.com.
Хост ресурса	URL, откуда будут получены события. По умолчанию применяется адрес https://manage.office.com.
Интервал ретроспективного анализа, часы	Период, за который запрашиваются все новые события, в часах. Для избежания потери некоторых событий важно задавать перекрывающиеся интервалы получения событий, так как некоторые типы контента Microsoft 365 могут передаваться с задержкой. При этом ранее полученные события не дублируются. По умолчанию запрашиваются все новые события за последние 12 часов.
Время ожидания ответа, сек	Период ожидания ответа на запрос на получение новых событий в секундах. По умолчанию время ожидания ответа составляет 30 секунд.

Параметр	Описание
Интервал повтора, сек	Время, через которое необходимо повторить запрос на получение новых событий в случае ошибки, в секундах. По умолчанию запрос на получение новых событий повторяется через 10 секунд после получения ошибки или при отсутствии ответа в течение заданного времени ожидания.
Интервал очищения, сек	Периодичность удаления устаревших данных в секундах. Минимальное значение – 300 секунд. По умолчанию устаревшие данные удаляются каждые 1800 секунд.
Интервал запросов, мин	Периодичность отправки запросов на получение новых событий в минутах. По умолчанию запросы отправляются каждые 10 минут.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к Microsoft 365. Можно выбрать один из доступных или создать новый прокси-сервер.

Коннектор, тип dfi

Коннекторы с типом **dfi** используются для получения данных Kaspersky Digital Footprint Intelligence по API. Доступные параметры коннектора с типом **dfi** 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.
Тип	Тип коннектора – **dfi**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

URL	URL-адрес API сервиса Kaspersky Threat Intelligence Portal. В URL-адресе вам нужно указать имя хоста и номер порта или только имя хоста. Вы можете указать только один URL-адрес. Адрес Kaspersky TIP: https://tip.kaspersky.com/api.
	Поддерживаются следующие форматы URL-адресов:
	• `имя хоста : номер порта` или `имя хоста`;
	Примеры:
	`http://tip_hostname:2134/api`
	`http://tip_hostname/api`
	• `IPv4-адрес : номер порта` или `IPv4-адрес`;
	Примеры:
	`http://127.0.0.1:2134/api`
	`http://127.0.0.1/api`
	• `[ IPv6-адрес ]: номер порта` или `[ IPv6-адрес ]`.
	IPv6-адрес должен быть указан в квадратных скобках. Примеры:
	`http://[1050:0:0:0:5:600:300c:326b]:2134/api`
	`http://[1050:0:0:0:5:600:300c:326b]/api`.
	KUMA не позволяет сохранить ресурс или сервис, если в поле URL есть знак табуляции или пробел.
	Обязательный параметр.

Параметр	Описание
Секрет	Секрет, в котором хранятся учетные данные для подключения к серверу Kaspersky Threat Intelligence Portal. Вы можете выбрать существующий секрет или создать новый секрет. Для создания секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша . **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В поле **Токен** укажите API-токен для аутентификации на портале Kaspersky Threat Intelligence Portal. Подробную информацию о получении API-токена вы найдете в справке Kaspersky Threat Intelligence Portal . 3. При необходимости с поле **Теги** добавьте теги для маркировки секрета. 4. При необходимости в поле **Описание** введите описание секрета. 5. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Интервал запросов	Интервал запросов к сервису Kaspersky Digital Footprint Intelligence, в секундах. Укажите число от 60 до 3600 (то есть от 1 минуты до 60 минут). Значение по умолчанию: `120`. Обязательный параметр.
Начальная временная метка	Дата и время, начиная с которого сервис Kaspersky Digital Footprint Intelligence сформирует данные по запросу. По умолчанию запрос в Kaspersky Digital Footprint Intelligence формируется с данными за последние 30 дней до момента запуска коллектора. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу Kaspersky Threat Intelligence Portal. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип universalAPI

Коннекторы с типом **universalAPI** используются для получения данных из любых REST API, поддерживающих ответы в формате JSON.

Коннектор этого типа предназначен для работы только с теми REST API, которые могут быть сконфигурированы средствами пользовательского интерфейса. В рамках одного коннектора можно создать только одно соединение. В рамках одного соединения можно настроить только один URL-адрес.

Для коннекторов типа **universalAPI** обычно используется нормализатор **json**. Однако такие коннекторы могут принимать ответы API не только в виде структуры JSON, но и в виде обычной строки или числа. Для обработки таких ответов вы можете использовать другие нормализаторы, например **regexp** или **kv**.

Коннектор **universalAPI** поддерживает сбор событий из структур JSON только с одним уровнем вложенности. Если структура ответа содержит вложенные списки (например, список объектов, внутри которых находится другой список объектов), сбор событий из таких списков средствами коннектора не поддерживается. В этом случае рекомендуется собирать данные верхнего уровня, а обработку вложенных структур выполнять на уровне нормализатора.

Коннектор **universalAPI** не передает в нормализатор пустые события, содержащие объект `{}` или `[]`.

Проверку соединения с источником можно выполнить после запуска коллектора, проанализировав его журналы. В случае возникновения проблем с соединением или авторизацией коллектор будет отображаться в разделе **Ресурсы** → **Активные сервисы** в желтом статусе.

> Коннектор с типом **universalAPI** не заменяет собой другие существующие API-коннекторы, например **office365**.

Доступные параметры коннектора с типом **universalAPI** 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.
Тип	Тип коннектора – **universalAPI**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес REST API сервера. Указывать протокол подключения (http или https) не нужно. Он определяется автоматически в зависимости от значения параметра `tlsMode`. Вы можете указать только один URL-адрес. Обязательный параметр.
Интервал запросов (сек.)	Интервал опросов заданного URL, в секундах. Укажите число от `60` до `86 400` (то есть от 1 минуты до 24 часов). Значение по умолчанию: `3600`.
HTTP метод	HTTP-метод запроса к API. Доступные значения: • **GET**. • **POST**. • **PUT**. • **DELETE**. Обязательный параметр.
Авторизация	Способ авторизации для подключения к API. Доступны следующие способы авторизации: • **Выключена**. Авторизация не используется. • **Обычная**. Авторизация по логину и паролю. Нужно использовать секрет типа **credentials**. • **Токен**. Авторизация по токену. Нужно использовать секрет типа **token**. Подробную информацию можно найти в разделе о секретах. Значение по умолчанию: **Выключена**. Если на вкладке **Дополнительные параметры** в поле **Режим TLS** выбрано значение **Нестандартный PFX**, поле **Авторизация** будет недоступно.
Идентификатор секрета	Поле доступно, если в поле **Авторизация** выбрано значение **Обычная**. Нужно выбрать секрет типа **credentials**. Обязательный параметр.
Токен	Поле доступно, если в поле **Авторизация** выбрано значение **Token**. Нужно выбрать секрет типа **token**. Обязательный параметр.

Параметр	Описание
Название токена	Поле доступно, если в поле **Авторизация** выбрано значение **Token**. Доступные значения: • **Bearer**. • **OAuth**. Вы также можете указать название вручную. Обязательный параметр.
Тело запроса	Тело HTTP-запроса. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`.
Путь к данным в формате JSONPath	Путь к данным в структуре ответа API, указывающий на объект или список объектов. Путь задается в формате JSONPath (например, `$.data`, `$.data.edges[0].node.event`, `$.data.edges[*].node.event`). Если в ответе API ожидается обычная строка или число, укажите в качестве пути символ `$`. Если при этом будет выключен параметр **Поле Identity** и не будут настроены параметры итераций, то данные будут переданы в нормализатор без изменения. Обязательный параметр.
Поле Identity	Переключатель для включения уникального идентификатора, по которому будут отбираться события. По умолчанию переключатель выключен.
Путь к полю в формате JSONPath	Поле доступно, если переключатель **Поле Identity** включен. Путь к полю идентификатора в структуре элемента данных ответа API задается в формате JSONPath (например, `$.id`). Обязательный параметр.
Тип	Поле доступно, если переключатель **Поле Identity** включен. Тип поля идентификатора, по которому будут отбираться события. Доступные значения: • **int**. • **float**. • **string**. • **date**. Внутри системы значение хранится в виде метки времени в миллисекундах. Обязательный параметр.
Формат даты	Поле доступно, если в поле **Тип** выбрано значение **date**. Формат даты может содержать дату, время, доли секунды и временную зону, например `YYYY-MM-DDTHH:mm:ssX`. Заданный формат применяется: • Для парсинга начального значения идентификатора. • Для парсинга значений идентификатора из ответов REST API. Если формат даты содержит временную зону, значение обрабатывается в указанной временной зоне. Если формат даты не содержит временную зону, значение обрабатывается в UTC. • Для формирования строки даты для параметров запроса (например, `$identityValue` в `queryParams`, `headers`, `body`). Если формат даты содержит временную зону, строка формируется во временной зоне сервера. Если формат даты не содержит временную зону, строка формируется в UTC.
Начальное значение	Поле доступно, если переключатель **Поле Identity** включен. Начальное значение поля идентификатора задается в виде строки в формате, соответствующем выбранному типу в поле **Тип**. Для типа **date** нужно указать значение в формате, указанном в поле **Формат даты**. Значение может содержать символы Unicode. Минимальная длина – 1 символ.
Параметры итераций	Переключатель для включения режима итераций, используемого для API с поэтапной выдачей данных. По умолчанию переключатель выключен.
Путь к полю с ключом итерации в формате JSONPath	Путь к полю ключа итерации в структуре элемента ответа API в формате JSONPath. Обязательный параметр.
Интервал запросов в режиме итераций (сек.)	Интервал опроса URL в режиме итерации, в секундах. Максимальное значение: `86 400` (24 часа). Значение по умолчанию: `60`.
Параметр URL для ключа итерации	Имя параметра URL, в котором передается ключ итерации при запросе к API.

Параметр	Описание
Необязательные параметры запроса	Дополнительные параметры запроса в формате `map[string][]string`. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`. Для добавления параметра нажмите на кнопку **+ Добавить** и заполните поля **Ключ** и **Значение**. Для удаления параметра установите рядом с ним флажок и нажмите на кнопку **Удалить**. Если включена итерация и в состоянии есть ключ итерации, он автоматически подставляется в параметры запроса.
Заголовки запроса	Опциональные заголовки HTTP-запроса в формате `map[string][]string`. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`. Для добавления параметра нажмите на кнопку **+ Добавить** и заполните поля **Ключ** и **Значение**. Для удаления параметра установите рядом с ним флажок и нажмите на кнопку **Удалить**.
Дополнительные поля	Дополнительные поля, которые добавляются в каждый элемент данных, в формате `map[string][]string`. Для добавления полей нажмите на кнопку **+ Добавить** и заполните поля **Название поля** и **JSONPath**. Для удаления поля установите рядом с ним флажок и нажмите на кнопку **Удалить**.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий режим отладки для коннектора. По умолчанию выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к API. Можно выбрать один из доступных прокси или создать новый.

Параметр	Описание

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.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра KUMA (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 хоста центра сертификации >" -out ca.crt`
	3. Создайте приватный 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 KUMA >" -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 KUMA в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс KUMA в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **Нестандартный PFX** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать 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**.

Время ожидания запроса (сек.)	Период ожидания ответа на запрос к API, в секундах. По умолчанию время ожидания ответа составляет 30 секунд.
Количество повторных запросов	Количество повторных попыток выполнить запрос при появлении ошибки. Значение по умолчанию: `1`.
Интервал повторных запросов (сек.)	Интервал между повторными попытками запроса, в секундах. Значение по умолчанию: `0`.

Предустановленные коннекторы

В поставку KUMA включены перечисленные в таблице предустановленные коннекторы.

Предустановленные коннекторы

Название коннектора	Комментарий
[OOTB] Continent SQL	Собирает события из СУБД АПКШ Континент. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] InfoWatch Person Monitor SQL	Собирает системные события аудита из СУБД MS SQL системы InfoWatch Person Monitor версии 10.2.
[OOTB] InfoWatch Traffic Monitor SQL	Собирает события из СУБД системы InfoWatch Traffic Monitor. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Kaspersky Security for MS Exchange Server SQL	Собирает события из СУБД MS SQL системы Kaspersky Security для Microsoft Exchange Servers версии 9.0. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MSSQL	Собирает события из СУБД MS SQL системы Kaspersky Security Center. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MySQL	Собирает события из СУБД MySQL системы Kaspersky Security Center. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC PostgreSQL	Собирает события из СУБД PostgreSQL системы Kaspersky Security Center версии 15.0. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Oracle Audit Trail SQL	Собирает события аудита из СУБД Oracle. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Parsec ParsecNet MSSQL	Собирает события из СУБД MS SQL системы ParsecNET 3. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] SecretNet SQL	Собирает события из СУБД системы SecretNet SQL. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] TeamPass MySQL	Собирает события из СУБД MySQL системы TeamPass версии 3.1.
[OOTB] Zabbix MySQL	Собирает события из СУБД MySQL системы Zabbix версии 6.4.

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, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

Секрет, созданный внутри ресурса в тенанте Shared, не отображается в разделе **Ресурсы и сервисы** → **Секреты** и недоступен для просмотра, в том числе пользователю с ролью Главный администратор. Такой секрет доступен для просмотра и действий только внутри ресурса, в котором создан.

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. Должно содержать от 1 до 128 символов в кодировке Unicode.
- **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 в кодировке Unicode.

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, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.
- **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.

    > Сертификат, включенный в PFX-файл, не может быть зашифрован алгоритмом AES-128-CBC. KUMA не поддерживает такие сертификаты.

  - **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 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.

- **fingerprint** – тип секрета используется для хранения значения **Elastic fingerprint**, которое может использоваться при подключении к серверу Elasticsearch.

- **PublicPKI** – тип секрета используется для подключения коллектора KUMA к ClickHouse. При выборе этого варианта требуется указать секрет, содержащий закрытый ключ PEM, закодированный в base64, и открытый ключ.

Предустановленные секреты

В поставку KUMA включены перечисленные в таблице ниже секреты.

Предустановленные секреты

Название секрета	Описание
[OOTB] Continent SQL connection	Хранит конфиденциальные данные и параметры подключения к БД системы АПКШ Континент. Для использования необходимо указать логин и пароль БД.
[OOTB] InfoWatch Person Monitor MS SQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL системы InfoWatch Person Monitor. Для использования необходимо указать логин и пароль БД.
[OOTB] InfoWatch Traffic Monitor SQL Connection	Хранит конфиденциальные данные и параметры подключения к БД системы InfoWatch Traffic Monitor. Для использования необходимо указать логин и пароль БД.
[OOTB] Kaspersky Security for Exchange SQL connection	Хранит конфиденциальные данные и параметры подключения к БД системы Kaspersky Security для Microsoft Exchange Servers. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MSSQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL системы Kaspersky Security Center. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MySQL Connection	Хранит конфиденциальные данные и параметры подключения к БД MySQL системы Kaspersky Security Center. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC PostgreSQL connection	Хранит конфиденциальные данные и параметры подключения к БД PostgreSQL системы Kaspersky Security Center. Для использования необходимо указать логин и пароль БД.
[OOTB] Oracle Audit Trail SQL Connection	Хранит конфиденциальные данные и параметры подключения к БД системы Oracle. Для использования необходимо указать логин и пароль БД.
[OOTB] Parsec MSSQL connection	Хранит конфиденциальные данные и параметры подключения к БД MSSQL системы Parsec. 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.
[OOTB] TeamPass MySQL connection	Хранит конфиденциальные данные и параметры подключения к БД MySQL системы TeamPass. Для использования необходимо указать логин и пароль БД.
[OOTB] Zabbix audit MySQL	Хранит конфиденциальные данные и параметры подключения к БД MySQL системы Zabbix. Для использования необходимо указать логин и пароль БД.

Правила сегментации

В KUMA можно настроить *правила сегментации алертов*, то есть правила разделения однотипных корреляционных событий по разным алертам.

По умолчанию, если в корреляторе какое-то правило корреляции сработает несколько раз, все созданные в результате этого корреляционные события будут присоединены к одному алерту. Правила сегментации алертов дают возможность определить условия, при которых на основе таких однотипных корреляционных событий будут создаваться разные алерты. Это может пригодиться, если вы хотите разделить поток корреляционных событий, например, по количеству событий или объединить некоторых из событий, отличающиеся чем-то важным от других, в отдельный алерт.

Сегментация алертов настраивается в два этапа:

1. Создаются *правила сегментации*, в которых определяются условия, по которым будет разделяться поток корреляционных событий.

2. К правилам сегментации привязываются правила корреляции, в которых должны срабатывать правила сегментации.

Создание правила сегментации

Правила сегментации алертов используются для разделения однотипных корреляционных событий по разным алертам. Условия для корреляционных событий, по которым будут создаваться отдельные алерты, задаются в правилах сегментации.

Чтобы создать правило сегментации:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Правила сегментации**, выберите нужный тенант и нажмите на кнопку **Создать**.

   Откроется окно **Создание правила сегментации**.

2. В поле **Имя** укажите имя правила сегментации. Имя должно быть уникальным и содержать от 1 до 128 символов в кодировке Unicode.

3. При необходимости в раскрывающемся списке **Тенант** измените тенант, которому принадлежит правило сегментации.

4. В раскрывающемся списке **Тип** укажите тип правила сегментации. Доступные значения:

   - **По фильтру** – алерт создается, если корреляционные события соответствуют условиям фильтра, заданным в блоке параметров **Фильтр**.

     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**. В группы фильтров можно добавить другие группы условий и отдельные условия. Условия и группы можно менять местами, перетаскивая их с помощью значка ⠿, а также удалять с помощью значка ✕. Условия можно задать с помощью операндов и операторов:

     - Левый операнд и Правый операнд – используются для указания значений, которые будет обрабатывать оператор.

       В левом операнде указываются названия полей событий, которые обрабатывает фильтр.

В правом операнде можно выбрать тип значения **константа** или **список**, а также указать само значение.

- **Доступные операторы**

  - **=** – 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.

Также можно добавить фильтр в режиме кода. Для этого необходимо перейти на вкладку **Код** в блоке **Фильтр** и в поле ввода указать параметры фильтра. При вводе значений параметров поддерживается автодополнение в виде списка подсказок с возможными вариантами значений. Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl`** + **`Space`**.

> Обратите внимание, что режим кода позволяет использовать в списке подсказок все возможные значения для правил в KUMA. Некоторые из этих значений могут быть недопустимыми для правил сегментации (например, `activelist`, `dictionary`, `hasbit`).

- **По группирующим полям** – алерт создается, если корреляционное событие содержит поля событий, указанные в раскрывающемся списке **Группирующие поля правила корреляции**.

  Группирующие поля можно выбрать в раскрывающемся списке **Группирующие поля правила корреляции** с помощью флажков. Добавленные поля можно удалить, нажав на значок крестика около названия группирующего поля.

  Пример использования группирующих полей

  Правило, детектирующее сканирование сети, создаст только один алерт, даже если в сети есть несколько устройств, сканирующих сеть. Если создать правило сегментации алертов по группирующему полю событий `SourceAddress`, а затем привязать это правило сегментации к правилу корреляции, при срабатывании правила будут созданы алерты для каждого адреса, с которого происходит сканирование.

В этом примере, если правило корреляции называется "`Network. Possible port scan`", а в ресурсе правила сегментации в качестве шаблона именования алертов указано "`from {{.SourceAddress}}`", будут созданы алерты такого вида:

- `Network. Possible port scan (from 10.20.20.20)`
- `Network. Possible port scan (from 10.10.10.10)`

- **По количеству событий** – алерт создается, если количество корреляционных событий в предыдущем алерте превысило значение, указанное в поле **Количество корреляционных событий**.

5. В поле **Шаблон именования алертов** укажите шаблон, в соответствии с которым алерты, создаваемые по этому правилу сегментации, будут получать название. Значение по умолчанию: `{{.Timestamp}}`. В поле шаблона можно указывать текст, а также поля события в формате `{{.<название поля события>}}`. При формировании названия алерта вместо названия поля события будет подставляться его значение. Название алерта, созданного с помощью правил сегментации, имеет следующий формат: `<Название правила корреляции, создавшего алерт> <текст из поля шаблона именования алертов> <значение указанного поля события>`. Например, если сработавшее правило корреляции называется "`Connection. Insecure port usage`" и в шаблоне наименования правила сегментации указано `{{.Timestamp}}`, будут созданы алерты вида:

   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:56:43 UTC)`
   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:59:46 UTC)`

   Если выполнится несколько правил сегментации с разными шаблонами именования алертов, в названии алерта они будут перечислены через разделительную черту `" | "`.

6. При необходимости в раскрывающемся списке **Теги** выберите теги для правила сегментации событий.

7. При необходимости в поле **Описание** укажите описание правила сегментации. Вы можете указать до 4000 символов в кодировке Unicode.

Правило сегментации будет создано. Далее созданное правило сегментации нужно связать с правилом корреляции.

Привязка правил сегментации к правилам корреляции

Связи правила сегментации и правил корреляции создаются отдельно для каждого тенанта. Они отображаются в разделе **Параметры** → **Алерты** → **Сегментация** веб-интерфейса KUMA в таблице со следующими столбцами:

- **Тенант** – название тенанта, которому принадлежат правила сегментации.
- **Обновлено** – дата и время последнего обновления правил сегментации.
- **Выключено** – в этом столбце отображается метка, если правила сегментации выключены.

Чтобы привязать правило сегментации алерта к правилам корреляции:

1. Откройте раздел **Параметры** → **Алерты** → **Сегментация** веб-интерфейса KUMA.

2. Выберите тенант, для которого вы хотите создать правило сегментации:

   - Если у тенанта уже есть правила сегментации, выберите его в таблице.

   - Если у тенанта нет правил сегментации, нажмите **Добавить параметры для нового тенанта** и в раскрывающемся списке **Тенант** выберите нужный тенант.

   Отображается таблица с созданными связями правил сегментации и корреляции.

3. В блоке параметров **Связи правил сегментации** нажмите **Добавить** и укажите параметры правила сегментации:

   - **Название** (обязательно) – в этом поле укажите название правила сегментации. Должно содержать от 1 до 128 символов в кодировке Unicode.

   - **Тенанты и правила корреляции** (обязательно) – в этом раскрывающемся списке выберите тенант и принадлежащее ему правило корреляции, события которого вы хотите выделить в отдельный алерт. Можно выбрать более одного правила корреляции.

   - **Правило сегментации** (обязательно) – в этом блоке параметров требуется выбрать ранее созданное правило сегментации, в котором определены условия сегментации.

   - **Выключено** – установите этот флажок при необходимости выключить связь правила сегментации.

4. Нажмите **Сохранить**.

   Правило сегментации и правила корреляции связаны. Корреляционные события, создаваемые указанными правилами корреляции, будут объединены в отдельный алерт с названием, определенном в правиле сегментации.

Чтобы выключить связи правил сегментации и правил корреляции для тенанта:

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса KUMA и выберите тенант, правила сегментации которого вы хотите выключить.

2. Установите флажок **Выключено**.

3. Нажмите **Сохранить**.

   Связи правил сегментации и правил корреляции для выбранного тенанта выключены.

Контекстные таблицы

Контекстная таблица – это контейнер для массива данных, которые используются корреляторами KUMA при анализе событий по правилам корреляции. Вы можете создать контекстные таблицы в разделе **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 таблицы 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.

> Если во время работы с данными контекстной таблицы коррелятор выключен, то в интерфейсе отображается ошибка "Internal communication failed", сообщающая о том, что потеряно соединение с источником данных, а именно потеряно соединение с коррелятором.

При удалении записей из контекстных таблиц по истечении срока жизни записи 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 обрабатывать события и 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.
`Name`	`context table record expired`
`DeviceVendor`	`Kaspersky`
`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`	Имя 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 выпавшей записи в контекстной таблице, выпавшая запись контекстной таблицы будет записана в соответствующий тип события:
	например, S.<поле контекстной таблицы> = <значение контекстной таблицы>
	SA.<поле контекстной таблицы> = <массив значений контекстной таблицы>
	
	Записи контекстной таблицы типа boolean имеют следующий вид:
	S.<поле контекстной таблицы> = true/false
	SA.<поле контекстной таблицы> = false,true,false

Просмотр списка контекстных таблиц

Вы можете просмотреть полный список контекстных таблиц или список контекстных таблиц, привязанных к конкретному коррелятору.

Полный список контекстных таблиц

Чтобы просмотреть полный список контекстных таблиц,

в веб-интерфейсе KUMA выберите **Ресурсы** → **Ресурсы** → **Контекстные таблицы**.

Отобразится список **Контекстные таблицы**.

Список контекстных таблиц конкретного коррелятора

Чтобы просмотреть список контекстных таблиц коррелятора:

1. В веб-интерфейсе KUMA выберите **Ресурсы** → **Работа с сервисами** → **Активные сервисы**.
2. Установите флажок напротив коррелятора, для которого вы хотите просмотреть список контекстных таблиц.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть контекстные таблицы**.

   Отобразится список **Контекстные таблицы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя контекстной таблицы.
- **Записи** – количество записей в контекстной таблице.
- **Размер на диске** – размер контекстной таблицы.
- **Директория** – путь к контекстной таблице на сервере коррелятора KUMA.

Добавление контекстной таблицы

Чтобы добавить контекстную таблицу:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. В окне **Контекстные таблицы** нажмите на кнопку **Создать**.

   Откроется окно **Создание контекстной таблицы**.
4. В поле **Название** введите имя контекстной таблицы.
5. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
6. 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.
7. В раскрывающемся списке **Теги** выберите теги для создаваемой контекстной таблицы.

   В списке отображаются все доступные теги, созданные в тенанте ресурса и Общем тенанте. Вы можете 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.
8. В поле **Описание** введите любую дополнительную информацию.

   Вы можете использовать до 4000 символов в кодировке Unicode.

   Поле необязательно для заполнения.
9. На вкладке **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 таблицы должно быть ключевым. Имена у 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 тип	Да	—

Тип данных поля	Может быть ключевым полем	Комментарий
Временная метка	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	—
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).

10. Добавьте нужное количество строк контекстной таблицы.

> После сохранения контекстной таблицы изменить количество строк невозможно.

11. Нажмите на кнопку **Создать**.

Контекстная таблица будет добавлена.

После добавления контекстной таблицы привяжите ее к правилу корреляции в параметрах правила корреляции в разделе **Обновление контекстных таблиц**. После этого привяжите это правило корреляции к коррелятору.

После привязки правила корреляции к коррелятору в параметрах контекстной таблицы появится поле **Коррелятор** и раздел **Контент**, в котором вы можете работать с содержимым контекстной таблицы.

Просмотр параметров контекстной таблицы

Чтобы просмотреть параметры контекстной таблицы:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. 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. 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 веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. В окне **Контекстные таблицы** в списке выберите контекстную таблицу, параметры которой вы хотите изменить.
4. Укажите значения для следующих параметров:
   - **Название** – уникальное имя ресурса.
   - **Тенант** – тенант, которому принадлежит ресурс. Это поле недоступно для редактирования.
   - **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Указывается в секундах.
   - **Теги** – теги для поиска ресурса.
   - **Описание** – любая дополнительная информация о ресурсе.
   - **Коррелятор** – коррелятор, к которому привязано корреляционное правило, в котором используется контекстная таблица. Это поле недоступно для редактирования. Это поле появляется после привязки правила корреляции к коррелятору.

- **Контент** – содержимое контекстной таблицы. Этот раздел появляется после привязки правила корреляции к коррелятору.

  Как менять содержимое контекстной таблицы

  Чтобы наполнить контекстную таблицу вручную или поменять ее содержимое, вам доступны следующие операции:

  - Добавить, изменить или удалить строку в таблице;
  - Дублировать строку;

    Вместо создания новой строки вы можете дублировать выбранную строку, изменить значения полей и сохранить.
  - Экспортировать контекстную таблицу;
  - Импортировать контекстную таблицу.

5. Перейдите на вкладку **Схема**. На этой вкладке отображается 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.

6. Нажмите **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. Чтобы применить изменения (удаление таблицы), обновите параметры коррелятора: в разделе **Ресурсы** → **Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором и нажмите **Обновить параметры**.
7. Добавьте в коррелятор контекстную таблицу, в которой вы изменили параметры.
8. Чтобы применить изменения (добавление таблицы), обновите параметры коррелятора: в разделе **Ресурсы** → **Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором и нажмите **Обновить параметры**.
9. Адаптируйте в экспортированной таблице (см. шаг 1) поля, чтобы они соответствовали полям таблицы, которую вы загрузили в коррелятор на шаге 7.
10. Импортируйте адаптированные данные в контекстную таблицу.

Параметры контекстной таблицы изменены.

Дублирование параметров контекстной таблицы

Чтобы скопировать контекстную таблицу:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. Установите флажок рядом с контекстной таблицей, которую вы хотите копировать.
4. Нажмите на кнопку **Дублировать**.
5. Укажите нужные вам параметры.
6. 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 веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. 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.

4. Нажмите на кнопку **Удалить**.
5. Нажмите на кнопку **OK**.

Контекстные таблицы будут удалены.

Просмотр и поиск записей контекстной таблицы

Чтобы просмотреть список записей контекстной таблицы:

1. Перейдите к полному списку контекстных таблиц или к списку контекстных таблиц конкретного коррелятора.

2. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.

   Для поиска по таблице в поле **Поиск** введите значение ключа записи или значение поля. В списке записей контекстной таблицы отобразятся только те записи, в 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>. Мы рекомендуем уточнить условия поискового запроса.

Список записей 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. Формат даты и времени зависит от выбранного языка интерфейса решения:

  - 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`

  Если при создании контекстной таблицы в поле **Срок действия** было указано значение 0, записи этой контекстной таблицы хранятся 36000 дней (около 100 лет).

- **Последнее обновление** – дата и время обновления контекстной таблицы.

Добавление, изменение и удаление записей в контекстной таблице

Чтобы изменить содержимое контекстной таблицы:

1. Откройте контекстную таблицу, строки которой вы хотите изменить.

2. Выполните одно из следующих действий:

   - Чтобы добавить строку, нажмите на кнопку **Добавить**, затем укажите значения полей и нажмите на значок галочки (✓), чтобы сохранить изменения. Поля, указанные на вкладке **Схема** как ключевые, обязательны для заполнения.

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 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 тип	false
IP-адрес	"0.0.0.0"
Временная метка	0
Список целых чисел	[]
Список чисел с плавающей точкой	[]
Список строк	[]
Список логических типов	[]
Список временных меток	[]
Список IP-адресов	[]

- Чтобы изменить строку, в столбце **Действия** нажмите на значок карандаша (✎), затем укажите значения полей и нажмите на значок галочки (✓), чтобы сохранить изменения.

  Значение ключевого поля записи недоступно для редактирования. Вы можете изменить его с помощью операций экспорта и импорта записи.

  Значение полей типов **Временная метка** и **Список временных меток** должно быть больше или равно 0. Значение полей типов **IP-адрес** и **Список IP-адресов** должно соответствовать формату IPv4 или IPv6.

- Чтобы дублировать строку, выделите строку и нажмите на кнопку **Дублировать**, затем укажите значения полей и нажмите на значок галочки (✓), чтобы сохранить изменения.

- Чтобы удалить строку, в столбце **Действия** нажмите на значок мусорной корзины (🗑).

Контекстная таблица изменена.

Экспорт данных из контекстной таблицы

Чтобы экспортировать данные из контекстной таблицы:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы** → **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 выгрузки (ГГГГ-ММ-ДД)>_<время выгрузки (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 решения:
  - 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 указываются 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.

Импорт данных в контекстную таблицу

Чтобы импортировать данные в контекстную таблицу:

1. В веб-интерфейсе KUMA выберите раздел **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, 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.

Вы также можете импортировать данные в контекстную таблицу в окне редактирования параметров контекстной таблицы.

Пример расследования инцидента с помощью Kaspersky SIEM

Выявление атаки на IT-инфраструктуру организации с помощью решения Kaspersky SIEM состоит из следующих шагов:

1. Предварительная подготовка
2. Назначение алерта пользователю
3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта
4. Анализ информации об алерте
5. Проверка на ложное срабатывание
6. Определение критичности алерта
7. Создание инцидента

8. Расследование
9. Поиск связанных активов
10. Поиск связанных событий
11. Запись причин инцидента
12. Реагирование
13. Восстановление работоспособности активов
14. Закрытие инцидента

В описании шагов приводится пример действий по реагированию, которые мог бы выполнить аналитик при обнаружении инцидента в IT-инфраструктуре организации. Вы можете посмотреть описание и пример для каждого шага, перейдя по ссылке в его названии. Примеры относятся непосредственно к описываемому шагу.

Условия инцидента, для которого приводятся примеры, см. в разделе *Условия возникновения инцидента*.

Более подробную информацию о способах и инструментах реагирования вы можете посмотреть в документе *Руководство по реагированию на инциденты информационной безопасности*. На сайте Securelist "Лаборатории Касперского" вы также можете ознакомиться с дополнительными рекомендациями по выявлению инцидентов и реагированию.

Условия возникновения инцидента

Параметры компьютера (далее также "актива"), на котором произошел инцидент:

- ОС актива – Windows 10.
- Программное обеспечение актива – Kaspersky Endpoint Agent, Kaspersky Endpoint Security.

Параметры KUMA:

- Настроена интеграция с Active Directory, Kaspersky Security Center, Kaspersky Endpoint Detection and Response.
- Установлены правила корреляции *SOC_package* из комплекта поставки решения.

Злоумышленник, заметив незаблокированный компьютер администратора, выполнил следующие действия на этом компьютере:

1. Скачал вредоносный файл со своего сервера.
2. Выполнил команду для создания ключа реестра в ветви `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.
3. Добавил скачанный на первом шаге файл в автозапуск с помощью реестра.
4. Очистил журнал событий безопасности Windows.
5. Завершил сессию.

Шаг 1. Предварительная подготовка

Предварительная подготовка включает следующие этапы:

1. Мониторинг событий.

   Когда в KUMA создан и настроен коллектор, решение записывает события информационной безопасности, зарегистрированные на контролируемых элементах IT-инфраструктуры организации, в базу событий. Вы можете найти и просмотреть эти события.

2. Создание коррелятора и правил корреляции.

   При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, решение создает алерты. Если для нескольких событий срабатывает одно и то же правило корреляции, все эти события привязываются к одному алерту. Вы можете использовать правила корреляции из комплекта поставки и создавать их вручную.

3. Настройка отправки уведомлений об алерте на один или несколько адресов электронной почты.

   Если отправка уведомлений настроена, при получении нового алерта KUMA отправляет на указанный адрес или адреса электронной почты уведомление. В уведомлении отображается ссылка на алерт.

4. Добавление активов.

   Вы можете выполнить на активе действия по реагированию (например, заблокировать запуск файла), только если актив добавлен в KUMA.

   Для выполнения действий по реагированию необходима интеграция KUMA с Kaspersky Security Center и Kaspersky Endpoint Detection and Response.

   Пример
   В рамках предварительной подготовки аналитик выполнил следующие действия:

   - Установил и привязал к коррелятору правила корреляции *SOC_package* из комплекта поставки.
   - Настроил отправку уведомлений об алертах на свой адрес электронной почты.
   - Импортировал в KUMA активы из Kaspersky Security Center.

   Согласно условиям инцидента, после того, как администратор выполнил вход в свою учетную запись, был запущен вредоносный файл, который злоумышленник добавил в автозапуск Windows. От актива в KUMA поступили события из журнала событий безопасности Windows. Для этих событий сработали правила корреляции.

   В результате в базу алертов KUMA были записаны следующие алерты:

   - R223_Сбор информации о процессах.
   - R050_Очистка журнала событий Windows.R295_Манипуляции с системой непривилегированным процессом.
   - R097_Манипуляции с загрузочным скриптом.
   - R093_Изменение критичных веток реестра.

   В информации об алерте указаны названия правил корреляции, по которым были созданы алерты, и время первого и последнего событий, созданных при повторном срабатывании правил.

   На адрес электронной почты аналитика пришли уведомления об алертах. Аналитик перешел по ссылке на алерт *R093_Изменение критичных веток реестра* из уведомления.

Шаг 2. Назначение алерта пользователю

Вы можете назначить алерт себе или другому пользователю.

Пример
В рамках рассматриваемого инцидента аналитик назначает алерт себе.

Шаг 3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта

На этом этапе вам нужно просмотреть информацию об алерте и убедиться, что данные событий алерта соответствуют сработавшему правилу корреляции.

Пример
В названии алерта указано, что была изменена критичная ветвь реестра. В информации об алерте, в разделе **Связанные события** отображается таблица событий, относящихся к алерту. Аналитик видит, что в таблице записано одно событие, где указан путь к измененному ключу реестра, исходное и новое значение ключа. Следовательно, правило корреляции соответствует событию.

Шаг 4. Анализ информации об алерте

На этом этапе вам нужно проанализировать информацию об алерте, чтобы определить, какие данные требуется для дальнейшего анализа алерта.

Пример
Из информации об алерте аналитик узнает следующие данные:

- какой ключ реестра был изменен;
- на каком активе;
- имя учетной записи, под которой был изменен ключ.

Эту информацию можно просмотреть в информации о событии, вызвавшем создание алерта (**Алерты** → алерт *R093_Изменение критичных веток реестра* → **Связанные события** → событие 2022-08-23 17:27:05), в полях FileName, DeviceHostName, SourceUserName соответственно.

Шаг 5. Проверка на ложное срабатывание

На этом этапе вам нужно убедиться, что активность, по которой сработало правило корреляции, не является нормальной для IT-инфраструктуры организации.

Пример
На этом этапе аналитик проверяет, может ли обнаруженная активность быть легитимной в связи с нормальной работой системы (например, обновлением). В информации о событии видно, что под учетной записью пользователя с помощью утилиты *reg.exe* был создан ключ реестра. Также ключ реестра был создан в ветви `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, отвечающей за автозапуск программ при входе пользователя в систему. По этим данным можно определить, что активность не является легитимной и срабатывание не было ложным.

Шаг 6. Определение критичности алерта

При необходимости вы можете изменить уровень критичности алерта.

Пример
Аналитик присваивает алерту высокую степень критичности.

Шаг 7. Создание инцидента

Если в ходе выполнения шагов 3–6 становится понятно, что алерт требует расследования, вы можете создать инцидент.

Пример
Для проведения расследования аналитик создает инцидент.

Шаг 8. Расследование

Этот этап включает просмотр информации о связанных с инцидентом активах, учетных записях, алертах в информации об инциденте.

Информация о затронутых активах и учетных записях отображается на вкладке **Связанные активы** и **Связанные пользователи** в информации об инциденте.

Пример
Аналитик открывает информацию о затронутом в рамках инцидента активе (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → необходимый актив). В информации об активе видно, что актив привязан к категориям *Business impact/HIGH* и *Device type/Workstation*, которые являются критичными для IT-инфраструктуры организации.

Также в информации об активе могут быть полезны следующие данные:

- FQDN, IP-адрес и MAC-адрес актива.
- Время создания актива и последнего обновления информации.
- Количество алертов, с которыми этот актив связан.
- Категории, к которым привязан актив.
- Уязвимости актива.
- Информация об установленном программном обеспечении.
- Информация об аппаратных характеристиках актива.

Аналитик открывает информацию о связанной учетной записи пользователя (**Инциденты** → необходимый инцидент → **Связанные алерты** → ссылка с необходимым алертом → **Связанные пользователи** → учетная запись).

В информации об учетной записи могут быть полезны следующие данные:

- Имя пользователя.
- Имя учетной записи.
- Адрес электронной почты.
- Группы, в которых состоит учетная запись.
- Дата истечения пароля.
- Дата создания пароля.
- Время последнего неверного ввода пароля.

Шаг 9. Поиск связанных активов

Вы можете просмотреть алерты, которые происходили на связанных с инцидентом активах.

Пример
Аналитик проверяет другие алерты, которые происходили на связанных с инцидентом активах (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → необходимый актив → **Связанные алерты**). В окне с алертами можно настроить фильтрацию по времени или статусу, чтобы исключить устаревшие или уже обработанные алерты. По времени, в которое были записаны алерты актива, аналитик определяет, что эти алерты связаны между собой, поэтому их можно привязать к инциденту (отметить флажками необходимые алерты → **Привязать** → необходимый инцидент → **Привязать**).

Также аналитик находит связанные алерты для учетной записи и привязывает их к инциденту. Все связанные активы, которые были в новых алертах, также проверяются.

Шаг 10. Поиск связанных событий

Вы можете расширить расследование, выполнив поиск событий из связанных алертов.

События можно найти в базе событий KUMA вручную или выбрать любой из связанных алертов и в информации о нем нажать на кнопку **Найти в событиях** (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → **Найти в событиях**). Найденные события можно привязать к выбранному алерту, предварительно отвязав алерт от инцидента.

Пример

В результате поиска аналитику удалось найти событие *A new process has been created*, в котором была записана команда для создания нового ключа реестра. Исходя из данных события, аналитик обнаружил, что родительским процессом для `reg.exe` был `cmd.exe`. То есть злоумышленник запустил командную строку и выполнил команду в ней. В информации о событии была записана информация о файле *ChromeUpdate.bat*, для которого был выполнен автозапуск. Чтобы узнать происхождение этого файла, аналитик выполнил поиск событий по базе событий по полю `FileName = ‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’` и по маске доступа `%%4417` (тип доступа *WriteData (or AddFile)*):

```
SELECT * FROM 'events' WHERE DeviceCustomString1 like '%4417%' and FileName like
‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’ AND Device Vendor 'Microsoft' ORDER BY Timestamp DESC LIMIT 250
```

В результате поиска аналитик обнаружил, что файл был скачан из внешнего источника с помощью процесса `msedge.exe.` Это событие аналитик также привязал к алерту.

Произведя поиск связанных событий для каждого алерта инцидента, аналитик выявил всю цепочку атаки.

Шаг 11. Запись причин инцидента

Вы можете внести необходимую для расследования информацию в журнал изменений инцидента.

Пример

По результатам, полученным в ходе поиска связанных с инцидентом событий, аналитик выявил причины инцидента и записал результаты анализа в поле **Журнал изменений** в информации об инциденте, чтобы передать информацию другим аналитикам.

Шаг 12. Реагирование на инцидент

Вы можете выполнить следующие действия по реагированию:

1. Выполнить сетевую изоляцию актива.
2. Запустить антивирусную проверку.
3. Запретить запуск файла на активах.

Перечисленные действия доступны при интеграции KUMA с Kaspersky Security Center и Kaspersky Endpoint Detection and Response.

Пример

У аналитика есть информация о связанных с инцидентом активах и об индикаторах компрометации, которая поможет в выборе действий по реагированию.

В рамках рассмотренного инцидента рекомендуется выполнить следующие действия:

- Запустить внеплановую антивирусную проверку актива, на котором был добавлен файл в автозапуск.
  Задача антивирусной проверки запускается через Kaspersky Security Center.
- Изолировать актив от сети на время антивирусной проверки.
  Изоляция актива выполняется с помощью Kaspersky Endpoint Detection and Response.
- Поместить файл *ChromeUpdate.bat* в карантин и создать правила запрета на запуск этого файла на других активах организации.
  Правило запрета на запуск файла создается с помощью Kaspersky Endpoint Detection and Response.

Шаг 13. Восстановление работоспособности активов

После того как IT-инфраструктура будет очищена от следов присутствия злоумышленника, вы можете отключить правила запрета и сетевой изоляции активов в Kaspersky Endpoint Detection and Response.

Пример

После выполнения действий по расследованию, реагированию и очистке IT-инфраструктуры организации от следов атаки можно приступить к восстановлению работоспособности активов. Для этого можно отключить правила запрета на запуск файла и правила сетевой изоляции активов в Kaspersky Endpoint Detection and Response, если они не были отключены автоматически.

Шаг 14. Закрытие инцидента

После того как были приняты меры по очистке IT-инфраструктуры организации от следов присутствия злоумышленника, вы можете закрыть инцидент.

Аналитика

KUMA предоставляет обширную аналитику по данным, доступным решению из следующих источников:

- События в хранилище
- Алерты
- Активы
- Учетные записи, импортированные из Active Directory
- Сведения из коллекторов о количестве обработанных событий
- Метрики

Вы можете настроить и получать аналитику в разделах **Панель мониторинга**, **Отчеты**, **Состояние источников** веб-интерфейса KUMA. Для построения аналитики используются только данные из тенантов, к которым у пользователя есть доступ.

Формат даты зависит от языка локализации, выбранного в настройках решения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Работа с событиями

В разделе **События** веб-интерфейса KUMA вы можете просматривать полученные решением события, чтобы расследовать угрозы безопасности или создавать правила корреляции. В таблице событий отображаются данные, полученные после выполнения SQL-запроса.

События можно отправлять в коррелятор для ретроспективной проверки.

Формат даты события зависит от языка локализации, выбранного в настройках решения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

https://rutube.ru/video/61eaf7b9ba77f32ed778ed174a9693a9/

Фильтрация и поиск событий

По умолчанию в разделе **События** веб-интерфейса KUMA данные не отображаются. Для просмотра событий в поле поиска нужно задать SQL-запрос и нажать на кнопку **Выполнить запрос**. SQL-запрос можно ввести вручную или сформировать с помощью конструктора запросов.

В SQL-запросах поддерживается агрегирование и группировка данных.

Вы можете осуществлять поиск событий по нескольким хранилищам. Например, таким образом вы можете выполнять поиск событий, чтобы определить, где учетная запись блокируется, или на какой URL с каких IP-адресов был выполнен вход. Пример запроса для поиска событий заблокированной учетной записи:

```
SELECT * FROM `events` WHERE DestinationUserName = 'username' AND DeviceEventClassID =
'4625' LIMIT 250
```

Чтобы выполнить поиск событий по нескольким хранилищам, в разделе **События** в раскрывающемся списке в верхней правой части раздела установите флажки рядом с нужными хранилищами.

В списке отображаются следующие хранилища:

- Хранилища тенанта Main.
- Доступные хранилища тенантов, для которых выполняется одно из следующих условий:
  - Тенант, которому принадлежит хранилище, включен в фильтре тенантов и у пользователя есть права на чтение событий в этом тенанте.
  - У пользователя есть доступ к тенанту одной из партиции хранилища и права на чтение событий в этом тенанте.

    Например, если у вас есть доступ к тенанту коллектора, но нет доступа к тенанту хранилища, по умолчанию хранилище недоступного тенанта не отображается в списке доступных хранилищ. Если в коллектор доступного вам тенанта добавлена точка назначения в хранилище недоступного вам тенанта, после того как в партицию тенанта коллектора поступило событие, хранилище недоступного тенанта появится в списке хранилищ в разделе **События**.

В поле раскрывающего списка хранилищ в верхней правой части раздела **События** отображается название первого из выбранных хранилищ и количество выбранных хранилищ, их несколько. Вы можете навести курсор мыши на поле раскрывающегося списка, чтобы отобразить все выбранные хранилища. Если пространство в хранилище удалено, в раскрывающемся списке хранилищ отображается deleted<идентификатор удаленного пространства>, события доступны для поиска в течение срока TTL.

Тенанты, выбранные в фильтре тенантов, влияют на то, какие хранилища отображаются в раскрывающемся списке хранилищ. Если в фильтре тенантов вы выключите тенанты, хранилища которых вам доступны, эти хранилища не будут отображаться в раскрывающемся списке хранилищ. Если эти хранилища были выбраны в раскрывающемся списке хранилищ, флажки напротив них будут сняты и события из этих хранилищ не будут отображаться. Если в раскрывающемся списке хранилищ выбрано только одно хранилище не из Main тенанта и в выборе тенантов вы выключили тенант, к которому принадлежит выбранное хранилище, это хранилище не будет отображаться в списке хранилищ и KUMA автоматически изменит выбор на одно из хранилищ тенанта Main.

Допускается простой запрос по всем выбранным хранилищам, как в примере выше. Если при выполнении запроса недоступно хотя бы одно из выбранных хранилищ, KUMA вернет ошибку.

Ограничения для поиска событий по нескольким хранилищам:

- При выполнении запроса к нескольким хранилищам недоступен экспорт в TSV, ретроспективная проверка и запросы REST API.
- В SELECT могут быть только * и/или названия полей события. Алиасы, функции, выражения не допускаются.
- В ORDER BY могут быть также только поля события (без функций, констант или выражений). Если такого поля нет в списке полей SELECT, то поле будет добавляться автоматически при отправке на конкретный кластер. ORDER BY ClusterID задать невозможно.
- GROUP BY недоступно.

Сложные запросы с группировками и агрегацией допускаются для одного выбранного хранилища.

Вы можете добавить условия фильтрации в уже сформированный SQL-запрос в окне просмотра статистики, таблицы событий и области деталей событий:

- **Изменение запроса из окна статистики**

  *Чтобы изменить параметры фильтрации из окна **Статистика**:*

  1. Откройте область деталей **Статистика** одним из следующих способов:

     - В правом верхнем углу таблицы событий в раскрывающемся списке ••• выберите **Статистика**.

     - В таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**.

     В правой части окна откроется область деталей **Статистика**.

  2. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.

  3. С помощью значков плюса и минуса измените параметры фильтрации, выполнив одно из следующих действий:

     - Если вы хотите включить в выборку событий только события с выбранным значением, нажмите +.

     - Если вы хотите исключить из выборки событий все события с выбранным значением, нажмите —.

     В результате параметры фильтрации и таблица событий будут обновлены, а в верхней части экрана отобразится измененный поисковый запрос.

- **Изменение запроса из таблицы событий**

  Чтобы изменить параметры фильтрации из таблицы событий:

  1. В разделе **События** веб-интерфейса KUMA нажмите на любое значение параметра события в таблице событий.

  2. В открывшемся меню выберите один из следующих вариантов:

     - Если вы хотите оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.

     - Если вы хотите исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

     В результате параметры фильтрации и таблица событий обновляются, а в верхней части экрана отображается измененный поисковый запрос.

- **Изменение запроса из области деталей события**

  Чтобы изменить параметры фильтрации в области деталей события:

  1. В веб-интерфейсе KUMA в разделе **События** нажмите на нужное событие.

     В правой части окна откроется область деталей **Информация о событии**.

2. Измените параметры фильтрации, используя значки плюса или минуса:

   - Если вы хотите применить фильтр сразу и обновить таблицу событий, нажмите + или — рядом с нужными параметрами.

   - Если вы хотите продолжить изменение параметров фильтрации, удерживая клавишу **Ctrl**, нажмите + или —. В этом случае условие добавляется в тело запроса, но запрос не выполняется автоматически.

     При добавлении условия в запрос, в секцию WHERE добавляется выражение по выбранному параметру. При добавлении условий для нескольких параметров, выражения соединяются оператором AND. В секцию SELECT добавляется поле, по которому выполняется фильтрация, только в том случае, если в запросе не используется символ *.

     Пример:
     Исходный запрос:
     ```
     SELECT *
     FROM `events`
     ORDER BY Timestamp DESC
     LIMIT 250
     ```
     Все события выбираются без фильтров, последние 250 событий отображаются в порядке убывания по полю Timestamp.
     При добавлении новых условий с помощью комбинации клавиши **Ctrl** и значка + запрос выглядит следующим образом:
     ```
     SELECT *
     FROM `events`
     WHERE DeviceProduct = 'Windows' AND StartTime = 1755767943436
     ORDER BY Timestamp DESC
     LIMIT 250
     ```
     Условия добавлены в секцию WHERE с оператором AND. В секцию SELECT поля не добавляются, так как в этой секции используется символ *. При этом запрос не выполняется автоматически.

3. После того как вы добавите все необходимые условия фильтрации, выполните запрос одним из следующих способов:

   - Добавьте последнее условие, не удерживая клавишу **Ctrl**. Запрос выполнится автоматически.

   - Закройте область деталей события и выполните запрос вручную, нажав на кнопку **Выполнить запрос** или используя комбинацию клавиш **Ctrl+Enter**.

   Параметры фильтрации и таблица событий будут обновлены, а в верхней части экрана отобразится измененный поисковый запрос.

После изменения запроса все параметры запроса, включая добавленные условия фильтрации, переносятся в конструктор и строку поиска.

Параметры запроса, введенного вручную в строке поиска, при переключении на конструктор не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строке поиска, пока вы не нажмете на кнопку **Применить запрос** в окне конструктора.

В поле ввода SQL-запроса можно включить отображение непечатаемых символов.

События можно также фильтровать по временному периоду. Результаты поиска можно автоматически обновлять.

Конфигурацию фильтра можно сохранить. Существующие конфигурации фильтров можно удалить.

Функции фильтрации доступны пользователям всех ролей.

При обращении к некоторым полям событий с идентификаторами KUMA возвращает соответствующие им названия.

Подробнее об SQL см. в справке ClickHouse. Также об SQL-операторах и функциях, поддерживаемых в KUMA, см. использование операторов в KUMA и поддерживаемые функции.

Выбор хранилища

События, которые отображаются в веб-интерфейсе KUMA в разделе **События**, получены из хранилища (то есть кластера ClickHouse). В зависимости от потребностей вашей компании у вас может быть более одного хранилища, однако для получения событий необходимо указывать, события из какого именно хранилища вам требуются.

Чтобы выбрать хранилище, из которого вы хотите получать события,

В разделе **События** веб-интерфейса KUMA откройте раскрывающийся список хранилищ в верхней правой части раздела и выберите одно или несколько пространств одного или нескольких хранилищ.

В списке отображаются следующие пространства:

- Пространства, добавленные при создании сервиса хранилища.
- Пространство KUMA Default.
- Пространство KUMA Audit, если выбран тенант Main и если в этом пространстве есть хотя бы одно событие аудита.

KUMA отображает только те пространства, к которым у пользователя есть права доступа.

В таблице событий отображаются события из выбранных пространств. Имена выбранных пространств отображаются в раскрывающемся списке.

Если у вас есть права доступа к пространству, в котором хранятся события тенанта, к которому у вас нет прав доступа, то такое пространство будет отображаться в списке, но поиск по этому пространству производиться не будет.

Формирование SQL-запроса с помощью конструктора

В KUMA вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

Чтобы сформировать SQL-запрос с помощью конструктора:

1. В разделе **События** веб-интерфейса KUMA нажмите на кнопку .

   Откроется окно конструктора запросов.

2. 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 вам проще было просматривать результаты поиска, в раскрывающемся списке вы можете выбрать необходимые поля, тогда в таблице будут отображаться данные только для выбранных полей. Стоит учитывать, что Select * в запросе увеличивает длительность выполнения запроса, но избавляет от необходимости прописывать поля в запросе вручную.

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**.

Если вы используете в SQL-запросе функции агрегации, вы можете настроить отображение столбцов в таблице событий. После выполнения запроса без * столбцы придут в соответствие с запросом.

Если в запросе используется группировка или агрегирующие функции, радар показывает не одно число, которое пришло по запросу `SELECT max(BytesOut) FROM `events` LIMIT 250`, а распределение событий, из которых получается это число.

> В режиме расследования алерта при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

- **FROM** – источник данных. Выберите значение **events**.

- **WHERE** – условия фильтрации событий.

  Условия и группы условий можно добавить с помощью кнопок **Добавить условие** и **Добавить группу**. По умолчанию в группе условий выбрано значение оператора **И**, однако если на него нажать, оператор можно изменить. Доступные значения: **И**, **ИЛИ**, **НЕ**. Структуру условий и групп условий можно менять, перетаскивая выражения с помощью мыши за значок ⠿.

  Добавление условий фильтра:

  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 вам потребуется ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

  Условия фильтра и группы условий можно удалить с помощью кнопки ×.

- **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в SQL-запросе группировку данных, в списке событий будут отображаться пользовательские поля, указанные в запросе. Настройка столбцов таблицы в группе недоступна. В событиях группы можно настроить отображение столбцов.

  > В режиме расследования алерта при фильтрации по событиям, связанным с алертами, невозможно группировать возвращаемые данные.

- **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.

Значение по умолчанию – 250.

Если при фильтрации событий по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить запрос**.

   Текущий SQL-запрос будет перезаписан. В поле поиска отобразится сформированный SQL-запрос.

   Если вы хотите сбросить настройки конструктора, нажмите на кнопку **Запрос по умолчанию**.

   Если вы хотите закрыть конструктор, не перезаписывая существующий запрос, нажмите на кнопку × в верхней правой части окна создания запроса.

4. Для отображения данных в таблице нажмите на кнопку **Выполнить запрос**.

   Вы также можете запустить выполнение запроса в фоновом режиме. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и нажмите на кнопку **Запустить в фоне**. В этом случае происходит следующее:

   - Запрос будет добавлен в очередь на выполнение в фоновом режиме, и в разделе **Диспетчер задач** 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 **Диспетчер задач**.

   При необходимости вы можете отменить выполнение запроса. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **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.

Подробнее об SQL см. в справке ClickHouse. Также см. использование операторов в KUMA и поддерживаемые функции.

Создание SQL-запроса вручную

Вы можете вручную использовать строку поиска, чтобы создавать SQL-запросы любой сложности для фильтрации событий.

Чтобы сформировать SQL-запрос вручную:

1. Перейдите в раздел **События** веб-интерфейса KUMA.

   Откроется форма с полем ввода.

2. Введите SQL-запрос в поле ввода. Вам нужно использовать одинарные кавычки в запросах.

3. Нажмите на кнопку **Выполнить запрос**.

   Вы также можете запустить выполнение запроса в фоновом 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 **Диспетчер задач** 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 **Диспетчер задач**.

   При необходимости вы можете отменить выполнение запроса. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **Отменить запрос**. При отмене запроса автоматически создается событие аудита.

   При необходимости вы можете отфильтровать события в таблице по периоду.

Поддерживаемые функции и операторы

Функция	Описание
`SELECT`	Поля событий, которые требуется возвращать. Поддерживаются следующие функции и операторы: • Функции агрегации `count`, `avg`, `max`, `min` и `sum`. • Арифметические операторы `+`, `-`, `*`, `/`, `<`, `>`, `=`, `!=`, `>=` и `<=`. Вы можете комбинировать в SQL-запросе функции и операторы. Если вы используете в SQL-запросе функции агрегации, вы можете настроить отображение столбцов в таблице событий. После выполнения запроса без * столбцы придут в соответствие с запросом. Если в запросе используется группировка или агрегирующие функции, радар показывает не одно число, которое пришло по запросу `SELECT max(BytesOut) FROM `events` LIMIT 250`, а распределение событий, из которых получается это число.
`FROM`	Источник данных. При создании SQL-запроса в качестве источника данных вам нужно указать значение events.
`WHERE`	Условия фильтрации событий: • `AND`, `OR`, `NOT`, `=`, `!=`, `>`, `>=`, `<` и `<=`. • `IN`. • `BETWEEN`. • `LIKE`. • `ILIKE`. • `inSubnet`. • `match` – в SQL-запросах используется синтаксис регулярных выражений re2. Вам нужно дополнительно экранировать специальные символы с помощью обратной косой черты `\`.
`GROUP BY`	Поля событий или псевдонимы, по которым требуется группировать возвращаемые данные. Если вы используете в SQL-запросе группировку данных, в списке событий будут отображаться пользовательские поля, указанные в запросе. Настройка столбцов таблицы в группе недоступна. В событиях группы можно настроить отображение столбцов.
`ORDER BY`	Столбцы, по которым требуется сортировать возвращаемые данные. Возможные значения: • `DESC` – сортировка по убыванию. • `ASC` – сортировка по возрастанию.

Функция	Описание
`OFFSET`	Количество строк, которые требуется пропустить перед отображением результатов SQL-запроса.
`LIMIT`	Количество отображаемых в таблице строк. Значение по умолчанию: `250`. Если при фильтрации событий по пользовательскому периоду количество строк в результатах поиска превышает указанное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше**. Эта кнопка не отображается при фильтрации событий по стандартному периоду.

Примеры SQL-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 хостов, 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.

Если вы хотите указать в запросе специальный символ, вам требуется экранировать его, поместив перед ним обратную косую черту (\).

Пример:

```
SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250
```

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.

При создании нормализатора для событий вы можете выбрать, сохранять ли значения полей исходного события. Данные сохраняются в поле события **Extra**. Поиск событий по этому полю осуществляется с помощью оператора LIKE.

Пример:

```
SELECT * FROM `events` WHERE DeviceAddress = '00.00.00.000' AND Extra LIKE '%"app":"example"%' ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events для хостов с IP-адресом 00.00.00.000, на которых запущен процесс example, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

Если вы создали SQL-запрос вручную в строке поиска и затем переключились на конструктор, параметры SQL-запроса не перенесутся в конструктор. В этом случае вам потребуется создать SQL-запрос в конструкторе заново. SQL-запрос, созданный в конструкторе, не перезаписывает SQL-запрос, введенный в строке поиска, пока вы не нажмете на кнопку **Применить запрос** в окне конструктора. Если вы создали SQL-запрос в конструкторе и затем переключились на поисковую строку, параметры запроса перенесутся автоматически.

Используемые в поисковых запросах псевдонимы не должны содержать пробелов.

Подробнее об SQL см. в справке ClickHouse. Также см. поддерживаемые функции ClickHouse.

Сохранение истории запросов

В веб-интерфейсе KUMA в разделе **События** сохраняется персональная история поисковых SQL-запросов. Вы можете обращаться к истории запросов и быстро находить нужный выполненный вами запрос.

Запросы сохраняются в браузере. При смене браузера история запросов очищается. В истории хранятся 32 последних введенных вами запроса. Запросы отображаются с форматированием. Отображается дата и время выполнения запроса.

В истории запросов сохраняются только запросы с правильным синтаксисом.

Чтобы найти поисковый запрос в истории:

1. В разделе **События** поместите курсор в строку запроса.
2. Нажмите мышкой на кнопку (**История SQL-запросов**), которая размещается на панели инструментов окна ввода запросов, или используйте комбинации клавиш **Ctrl+]** или **Ctrl+[** на клавиатуре.

   Откроется окно истории запросов. Вверху списка запросов отображается последний выполненный вами запрос.
3. Выберите поисковый запрос. Для навигации по списку сохраненных запросов используйте комбинацию клавиш **`Ctrl`**+**`]`** или **`Ctrl`**+**`[`**.

   Выбранный запрос подставится в строку запроса.
4. При необходимости выполните поисковый запрос. Для этого нажмите комбинацию клавиш **`Ctrl`**+**`Enter`**.

При выполнении запроса окно истории запросов закрывается.

Также окно с историей запросов вы можете закрыть, нажав на клавишу **`Esc`**, при этом курсор переместится в окно редактирования запроса.

Вы можете скопировать запрос в буфер обмена, нажав комбинацию клавиш **`Ctrl`**+**`C`**. При этом скопируется часть запроса, выделенная мышкой, или вся строка запроса, ограниченная рамкой, если не было выделения.

Вы можете сохранить запрос нажав комбинацию клавиш **`Ctrl`**+**`S`**, либо нажав мышкой на кнопку (**Сохранить запрос**) в строке. При этом окно истории закроется, и откроется боковая панель для сохранения запроса с заполненными полями.

Пользователь может вставить запрос в окно запроса без выполнения, нажав мышкой на кнопку (**Вставить запрос**), либо на клавишу **`Enter`**.

Работа с сохраненными поисковыми запросами

В KUMA в разделе **События** вы можете организовать сохраненные SQL-запросы в дереве папок для структурированного хранения и быстрого поиска SQL-запросов. Вы можете редактировать ранее сохраненные запросы, переименовывать их, размещать запросы в группах (папках) доступных тенантов и осуществлять поиск по ранее сохраненным запросам в поисковой строке.

Сохраненные запросы подчиняются тенантной модели доступа и будут видны всем пользователям, которые имеют доступ к соответствующим тенантам.

Сохраненные запросы размещаются в панели **Сохраненные запросы.** Вы можете открыть или закрыть панель **Сохраненные запросы** с помощью кнопки (закладка) в панели инструментов окна ввода запросов.

Навигационная панель **Сохраненные запросы** отображается слева и содержит:

- Окно поиска запроса, в котором вы можете выполнять поиск по имени папки и имени запроса.
- Дерево папок и запросов, папку **Избранное.**
- Фильтр запросов: отображение запросов, созданных вами (вкладка **Мои**) и отображение всех запросов (вкладка **Все**).

Отображение запроса в окне запросов

Чтобы отобразить запрос в окне запросов:

1. В разделе **События** нажмите на кнопку (закладка).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** мышкой выберите нужный запрос.

Текст выбранного запроса отображается в окне запросов.

Сохранение запроса в папку или тенант

В разделе **События** после введения запроса в окне запросов и нажатия на кнопку **Сохранить текущий запрос** (значок дискеты) вы можете сохранить SQL-запрос в доступную для выбора папку или тенант.

Чтобы сохранить запрос в папку:

1. В окне **Новый запрос** в поле **Название фильтра** введите название фильтра.

   При вводе названия фильтра учитывайте следующее:

   - Название содержит символы Unicode.
   - Минимальная длина названия – 1 символ, максимальная – 128 символов.
   - В одном тенанте не может быть одинаковых названий.
   - Символы табуляции, переноса строки и красной строки заменяются на символ пробела.

   При сохранении названия:

   - Пробелы в начале и конце строки удаляются.
   - Множественные пробелы между символами сокращаются до одного.

2. В поле **Запрос** введите текст SQL запроса.

3. Выберите тенант, папку из списка папок, созданных в доступном вам тенанте, или создайте новую папку, нажав на кнопку **Добавить папку**.

   Добавить папку вы также можете в окне **Сохраненные запросы**, нажав на кнопку + напротив тенанта и добавив папку в появившемся окне **Новая папка.**

4. Нажмите на кнопку **Сохранить**.

Запрос будет сохранен в выбранной папке или тенанте.

Просмотр текста запроса

Чтобы просмотреть текст запроса:

1. В разделе **События** нажмите на кнопку (закладка).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** напротив нужного запроса нажмите на кнопку .

Появляется окно с текстом запроса.

Установка запроса по умолчанию

Вы можете выбрать себе запрос по умолчанию, с которым будет открываться раздел **События**.

Чтобы установить запрос по умолчанию:

1. В разделе **События** нажмите на кнопку (закладка).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** выберите нужный запрос.

3. Нажмите на кнопку и в открывшемся меню выберите пункт **Использовать по умолчанию**.

Выбранный запрос будет использоваться по умолчанию.

Добавление папок и запросов в избранное

Чтобы добавить папку или отдельный запрос в избранное:

1. В разделе **События** нажмите на кнопку (закладка).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** выберите нужную папку или запрос.

3. Нажмите на кнопку и в открывшемся меню выберите пункт **В избранное**.

Выбранная папка или ресурс переместится в папку **Избранное**.

Редактирование запроса

Чтобы отредактировать запрос:

1. В разделе **События** нажмите на кнопку (закладка).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** выберите нужный запрос.

3. Нажмите на кнопку и в открывшемся меню выберите пункт **Изменить**.

   Откроется окно изменения сохраненного запроса.

4. В окне измените название, текст запроса или папку, в которой будет сохранен запрос.

5. Нажмите на кнопку **Сохранить**.

Запрос будет обновлен и сохранен в выбранной папке.

Удаление запроса

Чтобы удалить запрос из папки при наличии прав:

1. В разделе **События** нажмите на значок закладки ( ).

   Откроется навигационная панель **Сохраненные запросы**.

2. В дереве папок панели **Сохраненные запросы** выберите нужный запрос.

3. Нажмите на значок с тремя точками ( ) и в появившемся меню выберите пункт **Удалить**.

4. В открывшемся окне подтвердите удаление.

Запрос будет удален.

Фильтрация событий по периоду

В KUMA вы можете настроить отображение событий, относящихся к определенному временному периоду.

Чтобы отфильтровать события по периоду:

1. В разделе **События** веб-интерфейса KUMA в верхней части окна откройте раскрывающийся список временного периода в верхней правой части раздела.

2. Выберите период одним из следующих способов:

   - Если вы хотите указать **точную дату**, в календаре 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 выберете 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**.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите указать **пользовательский период**, задайте 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. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. 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 и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также 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.

По умолчанию выбрано значение **5 минут** (**now-5m**). 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.

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**, события 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 события 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, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

3. Если вы хотите зафиксировать последний относительный период, по которому выполнялся запрос, как точные дату и время, нажмите на кнопку 📌.

   После этого относительный период преобразуется в точные дату и время. Вы можете навести курсор мыши на эту кнопку, чтобы отобразить дату и время, которые будут зафиксированы. Относительные периоды **Сегодня**, **Вчера**, **Эта неделя**, **Этот месяц** преобразуются в точные дату и время в UTC, остальные периоды – в дату и время с учетом часового пояса браузера.

   > Если вы выполнили SQL-запрос с группировкой событий, то при переключении между группами в результатах запроса относительный временной диапазон автоматически преобразуется в точные дату и время.

4. Нажмите на кнопку **Выполнить запрос**.

   Отобразятся только события, зарегистрированные в течение указанного интервала времени. Период отобразится в верхней части окна.

Вы также можете настроить отображение событий с помощью гистограммы событий, которая отображается при нажатии на кнопку 📊 в верхней части раздела **События**. События отобразятся, если нажать на нужный столбец данных или выделить требуемый период времени и нажать на кнопку **Показать события**.

Отображение списка событий при относительном и точном календарном периоде

Отображение списка событий в таблице в разделе **События** зависит от того, какой период выбран для фильтрации событий: относительный или точный календарный.

Когда выбран относительный период, отображение осуществляется следующим образом:

- Если в SQL-запросе для переменной `LIMIT` указано определенное значение, то отображается количество событий, соответствующее этому значению.

  Пример SQL-запроса: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 10`.

- Если в SQL-запросе значение `LIMIT` не указано, по умолчанию отображается 250 событий.

  Пример SQL-запроса: `SELECT * FROM `events` ORDER BY Timestamp DESC`.

> Если выбран относительный период, события в KUMA отображаются без разбиения на страницы.

Когда выбран точный календарный период, отображение осуществляется следующим образом:

- Если в SQL-запросе для переменной `LIMIT` указано значение меньше или равно 49, а событий найдено больше 49, вы можете посмотреть в таблице дополнительные строки, нажав на кнопку **Показать больше**.

  Пример SQL-запроса: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 48`.

- Если в SQL-запросе для переменной `LIMIT` указано значение больше 49 и событий найдено больше 49, события в списке подгружаются автоматически.

  Пример SQL-запроса: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 50`.

Группировка событий

После получения списка событий часто возникает потребность разделить полученные события по группам, чтобы локализовать событие информационной безопасности. В KUMA есть возможность сгруппировать события по одному или нескольким полям для полученного списка событий.

Чтобы сгруппировать события, теперь не нужно вручную корректировать текст запроса - можно в разделе **События** нажать на заголовок столбца и в контекстном меню выбрать **Добавить GROUP BY в запрос**. Вы можете выбрать последовательно несколько полей для группировки, поля будут автоматически добавлены в строку запроса. После того как вы выбрали нужные поля, нажмите **Выполнить запрос**. В результате будет выполнена группировка событий по заданным полям. Найденные группы будут отображаться в разделе **Группы**. Отображение доступно в виде таблицы и в виде карточек. Вы можете переключаться между режимами отображения.

Можно исключить группу из запроса:

- В режиме **Карточки** нажмите на значок минус (`—`).

- В режиме **Таблицы** нажмите правой кнопкой мыши по группе и в появившемся контекстном меню выберите **Исключить группу из фильтра**.

В результате запрос автоматически изменится и группа будет исключена из запроса.

Если вы хотите вернуться к исходному запросу, нажмите **Вернуться к исходному запросу**.

По группам можно переходить и просматривать содержимое каждой группы.

Доступен глобальный поиск по всем группам и локальный поиск по событиям в рамках выбранной группы.

Можно усложнить группировку и добавить одно или несколько полей.

Можно удалить группу из группировки и таким образом вернуться на шаг назад.

Если запрос по группе возвращает много событий, будут отображаться только первые 1000 событий. Если в запросе содержится SELECT Count(ID), можно перейти по ссылке, которой является общее количество событий в результате запроса, и посмотреть все события. Если запрос не содержит Count(ID), количество событий в группе указано не будет, но сохраняется возможность перейти по ссылке и посмотреть общее количество событий в группе.

Доступна статистика, ретроспективное сканирование по группам и Экспорт в TSV.

Если вы хотите, чтобы результат группировки не зависел от времени – поскольку события поступают постоянно - вы можете зафиксировать относительный интервал и применить его как абсолютный, чтобы интересующие вас события не выпали из выборки. Чтобы зафиксировать относительный интервал, в разделе **События** в раскрывающемся списке с временным интервалом выберите **Применить текущий диапазон**. Теперь вы можете работать с группами в рамках этого запроса.

Если вы хотите распределить выбранные события по месяцам, дням, минутам и секундам, вы можете выполнить группировку событий по полю Timestamp. Чтобы выполнить группировку, в таблице событий в поле Timestamp в контекстном меню выберите нужную опцию группировки.

Если вы хотите нормализовать значение поля Timestamp и смотреть время из разных источников по одной шкале времени UTC, в таблице событий в поле Timestamp в контекстном меню выберите **Конвертировать в часовой пояс UTC**.

Отображение названий вместо идентификаторов

При обращении к некоторым полям событий, содержащих идентификаторы, KUMA возвращает не идентификаторы, а соответствующие им названия. Это сделано для удобства восприятия информации. Например, если вы обратитесь к полю события `TenantID` (в который записывается идентификатор тенанта), вы получите значение из поля событий `TenantName` (в которое записывается название тенанта).

При экспорте событий в файл записываются значения из обоих полей: и с идентификатором, и с названием.

В таблице ниже перечислены поля, при обращении к которым происходит замена:

Запрашиваемое поле	Поле, из которого возвращается значение
`TenantID`	`TenantName`
`ServiceID`	`ServiceName`
`DeviceAssetID`	`DeviceAssetName`
`SourceAssetID`	`SourceAssetName`
`DestinationAssetID`	`DestinationAssetName`
`SourceAccountID`	`SourceAccountName`
`DestinationAccountID`	`DestinationAccountName`

Замена не происходит, если в SQL-запросе полю присвоен псевдоним. Примеры:

- `SELECT TenantID FROM `events` LIMIT 250` – в результате поиска в поле TenantID будет отображаться название тенанта.
- `SELECT TenantID AS Tenant_name FROM `events` LIMIT 250` – в результате поиска в поле Tenant_name будет отображаться идентификатор тенанта.

Пресеты

Вы можете использовать пресеты для упрощения работы с запросами, если вы регулярно хотите просматривать данные по определенному набору полей событий. В строке с SQL-запросом можно ввести `Select *` и выбрать сохраненный пресет - выдача будет ограничена только указанными в пресете полями. Такой способ снижает производительность, но при этом избавляет от необходимости каждый раз писать запрос вручную.
Пресеты сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA для указанного тенанта.

Чтобы создать пресет:

1. В разделе **События** нажмите на значок ⚙.
2. В открывшемся окне на вкладке **Столбцы полей событий** выберите необходимые поля.

   Для упрощения поиска можно начать набирать название поля в области **Поиск**.
3. Чтобы сохранить выбранные поля, нажмите **Сохранить текущий пресет**.

   Откроется окно **Новый пресет**.
4. В открывшемся окне укажите **Название** пресета и выберите **Тенант** в раскрывающемся списке.
5. Нажмите **Сохранить**.

   Пресет создан и сохранен.

Чтобы применить пресет:

1. В поле ввода запроса введите **Select ***.
2. В разделе **События** веб-интерфейса KUMA нажмите на значок ⚙.
3. В открывшемся окне на вкладке **Пресеты** выберите нужный пресет и нажмите на кнопку ⇥.

   Поля из выбранного пресета будут добавлены в поле с SQL-запросом, а столбцы будут добавлены в таблицу. В конструкторе запросов изменений не произойдет.
4. Нажмите на кнопку **Выполнить запрос**, чтобы выполнить запрос.

   После выполнения запроса столбцы будут заполнены.

Ограничение сложности запросов в режиме расследования алерта

При расследовании алерта сложность SQL-запросов для фильтрации событий ограничена, если при расследовании алерта в раскрывающемся списке источников событий выбрано значение **События алерта**. В этом случае для фильтрации событий доступны только перечисленные ниже функции и операторы.

> При выборе в раскрывающемся списке источников событий значения **Все события** ограничения не действуют.

- `SELECT`
  - В качестве символа подстановки используется `*`.
- `WHERE`
  - `AND`, `OR`, `NOT`, `=`, `!=`, `>`, `>=`, `<`, `<=`
  - `IN`
  - `BETWEEN`

- `LIKE`
- `inSubnet`

Примеры:

- `WHERE Type IN ('Base', 'Correlated')`
- `WHERE BytesIn BETWEEN 1000 AND 2000`
- `WHERE Message LIKE '%ssh:%'`
- `WHERE inSubnet(DeviceAddress, '10.0.0.1/24')`

- `ORDER BY`

  Сортировка возможна по столбцам.

- `OFFSET`

  Пропуск указанного количества строк перед выводом результатов запроса.

- `LIMIT`

  Значение по умолчанию – 250.

  Если при фильтрации событий по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше**. Кнопка не отображается при фильтрации событий по стандартному периоду.

В режиме расследования алерта при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

Сохранение и выбор конфигураций фильтра событий

В KUMA вы можете сохранять конфигурации фильтров для использования в будущем. Другие пользователи также могут использовать сохраненные фильтры при условии, что у них есть соответствующие права доступа. При сохранении фильтра вы сохраняете настроенные параметры сразу всех активных фильтров: фильтр по периоду, конструктору запросов и параметры таблицы событий. Поисковые запросы сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA выбранного тенанта.

Чтобы сохранить текущие настройки фильтра, запроса и периода:

1. В разделе **События** веб-интерфейса KUMA нажмите на значок рядом с выражением фильтра.

   Откроется окно **Новый фильтр**.

2. В открывшемся окне в поле **Название** введите название конфигурации фильтра. Название должно содержать до 128 символов в кодировке Unicode.

3. В блоке **Выберите папку** выберите тенант, которому будет принадлежать создаваемый фильтр, и папку внутри тенанта при необходимости.

   Для упрощения поиска можно начать набирать название в области **Поиск**.

4. При необходимости нажмите на кнопку **Добавить папку**, чтобы создать новую папку внутри выбранного тенанта.

5. Нажмите **Сохранить**.

   Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

в разделе **События** веб-интерфейса KUMA нажмите на значок ☆ рядом с выражением фильтра и выберите нужный фильтр.

Выбранная конфигурация активна: в поле поиска отображается поисковый запрос, в верхней части окна настроенные параметры периода и частоты обновления результатов поиска. Для отправки поискового запроса нажмите на кнопку **Выполнить запрос**.

Если навести курсор на название конфигурации фильтра, нажать на значок ⋮ рядом с названием конфигурации и нажать на кнопку **В избранное**, конфигурация фильтра будет добавлена в избранное.

Удаление конфигураций фильтра событий

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе **События** веб-интерфейса KUMA нажмите на значок ☆ рядом с поисковым запросом фильтра.

   Откроется окно **Сохраненные запросы**.

2. Наведите курсор мыши на конфигурации, которую требуется удалить, и нажмите на значок ⋮ рядом с ее названием.

3. В открывшемся меню нажмите на значок 🗑.

   Конфигурация фильтра удалена для всех пользователей KUMA.

Поддерживаемые функции ClickHouse

В KUMA поддерживаются следующие функции ClickHouse:

- Арифметические функции.
- Массивы.
- Функции сравнения.
- Логические функции.
- Функции преобразования типов.
- Функции для работы с датами и временем.
- Функции для работы со строками.
- Функции поиска в строках.

- Условные функции: только обычный оператор if, тернарный оператор не поддерживается.
- Математические функции.
- Функции округления.
- Функции разбиения и слияния строк и массивов.
- Битовые функции.
- Функции для работы с UUID.
- Функции для работы с URL.
- Функции для работы с IP-адресами.
- Функции для работы с Nullable-аргументами.
- Функции для работы с географическими координатами.

Функции из остальных разделов не поддерживаются.

Подробнее об SQL см. в справке ClickHouse.

Просмотр информации о событии

Чтобы просмотреть информацию о событии:

1. В окне веб-интерфейса решения выберите раздел **События**.
2. Выполните поиск событий с помощью конструктора запросов или введя запрос в строке поиска.

   Отобразится таблица событий.
3. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

В правой части окна отображается область деталей **Информация о событии** со списком параметров события и их значений. В этой области деталей можно:

- Включить выбранное поле в поиск или исключить его из поиска, нажав на + и — рядом со значением параметра.
- По хешу файла в поле **FileHash** раскрыть список, в котором вы можете выбрать одно из следующих действий:
  - Показать информацию из **Threat Lookup**.

    Доступно при интеграции с **Kaspersky Threat Intelligence Portal**.
  - Добавить в **Internal TI CyberTrace**.

    Доступно при интеграции с **Kaspersky CyberTrace**.

- Открыть окно со сведениями об активе, если он упоминается в полях события и зарегистрирован в решении.

- По ссылке с именем коллектора в поле **Service** просмотреть параметры сервиса, зарегистрировавшего событие.

  Вы также можете привязать событие к алерту, если решение находится в режиме расследования алерта, и открыть окно **Информация о корреляционном событии**, если выбранное событие является корреляционным.

- Просмотреть все непустые поля события, нажав **Посмотреть все поля события**. При этом должны выполняться следующие условия:

  - Запрос выполнен по набору полей, а не SELECT *.

  - Показаны не все непустые поля. Если в карточке события показаны все непустые поля, кнопка **Посмотреть все поля события** отображаться не будет.

  - Карточка события открыта в KUMA в разделе **События**.

  При этом исходный запрос не меняется и таблица событий не перестраивается.

  Пример

  Предварительное условие:

  Отправлено событие с несколькими заполненными полями, например Message, SourceAddress, DeviceCustomString1.

  Выполнен запрос по набору полей.

```
SELECT Type, Message

FROM `events`

ORDER BY Timestamp

DESC LIMIT 250
```

  Если вы нажмете на событие, в открывшемся окне **Информация о событии** отобразятся следующие данные:

  - Поля Type и Message из запроса.

  - Отобразятся поля по умолчанию, не указанные в запросе – TenantID и Timestamp.

  Не будут отображаться заполненные поля SourceAddress и DeviceCustomString1, которые отсутствуют в запросе и при этом есть в отправленном событии.

  Если вы хотите просмотреть все непустые поля, нажмите **Посмотреть все поля события**.

Отобразятся все заполненные поля события: Type, Message, TenantID, Timestamp, SourceAddress, DeviceCustomString1.

- Изменить отображение события по кнопке **Форматировать**. По умолчанию событие отображается в виде однострочной записи в формате XML или JSON. При нажатии на кнопку оно отображается в виде многострочной записи с отступами. Повторное нажатие возвращает однострочный формат отображения. Форматирование применяется ко всем событиям в таблице в разделе **События**.

В области деталей **Информация о событии** в качестве значений перечисленных ниже параметров вместо идентификатора показывается название описываемого объекта. При этом, если изменить фильтрацию событий по этому параметру (например, нажать на значок —, чтобы исключить из результатов поиска события с определенной комбинацией параметр-значение), в SQL-запрос будет добавлен идентификатор объекта, а не его название:

- TenantID
- ServiceID
- DeviceAssetID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

Экспорт событий

Из KUMA можно экспортировать информацию о событиях в TSV-файл. Выборка событий, которые будут экспортированы в TSV-файл, зависит от настроек фильтра. Информация экспортируется из столбцов, которые в этот момент отображаются в таблице событий, при этом столбцы в файле наполняются доступными данными, даже если в таблице событий в веб-интерфейсе KUMA они не отображались из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. В разделе **События** веб-интерфейса KUMA нажмите на кнопку **TSV** в верхней части таблицы событий.

   Новая задача экспорта TSV-файла создается в разделе **Диспетчер задач**.

2. Найдите созданную вами задачу в разделе **Диспетчер задач**.

   Когда файл будет готов к загрузке, в строке задачи в столбце **Статус** отобразятся статус **Завершено** и значок ⊘.

3. Нажмите на название типа задачи и в раскрывающемся списке выберите **Загрузить**.

   TSV-файл с информацией о событиях будет загружен с использованием настроек вашего браузера. Имя файла по умолчанию: event-export-<date>_<time>.tsv.

Файл сохраняется в соответствии с настройками вашего веб-браузера.

Настройка таблицы событий

В разделе **События** отображаются ответы на SQL-запросы пользователя, представленные в виде таблицы. Поля, выбранные в пользовательском запросе, отображаются в конце таблицы, после столбцов по умолчанию. Таблицу можно обновлять.

Следующие столбцы в таблице событий отображаются по умолчанию:

- **TenantID**.
- **Timestamp**.
- **Name**.
- **DeviceProduct**.
- **DeviceVendor**.
- **DestinationAddress**.
- **DestinationUserName**.

В KUMA можно настроить отображаемый набор полей событий и порядок их отображения. Выбранную конфигурацию можно сохранить в пресет.

При использовании для фильтрации событий SQL-запросов с группировкой и агрегацией данных статистика недоступна, а состав и порядок столбцов зависит от SQL-запроса.

В таблице событий, в области деталей событий, в окне алертов, а также в виджетах в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Чтобы настроить поля, отображаемые в таблице событий:

1. В правом верхнем углу таблицы событий нажмите значок ⚙.

   Откроется окно для выбора полей событий, которые требуется отображать в таблице событий.

2. Установите флажки напротив полей, которые требуется отображать в таблице. С помощью поля **Поиск** можно найти нужные поля.

   Вы можете отобразить в таблице любое поле события из модели данных событий KUMA и расширенной схемы событий. Параметры **Timestamp** (Время) и **Name** (Название) всегда отображаются в таблице. С помощью кнопки **По умолчанию** можно вернуть исходные настройки отображения таблицы событий.

   Когда вы устанавливаете флажок, таблица событий обновляется и добавляется новый столбец. При снятии флажка столбец исчезает.

Столбец можно удалить из таблицы событий, если нажать на его заголовок и в раскрывающемся списке выбрать **Скрыть столбец**.

3. При необходимости измените порядок отображения столбцов, перетаскивая заголовки столбцов в таблице событий.

4. Если вы хотите сортировать события по определенному столбцу, нажмите на его заголовок и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

Выбранные поля событий отобразятся в таблице раздела **События** в качестве столбцов в указанном вами порядке.

Список выбранных полей хранится локально в настройках браузера. Чтобы унифицировать параметры отображения столбцов в разных браузерах или на разных устройствах, рекомендуется использовать пресеты.

Обновление таблицы событий

Таблицу событий можно обновлять, перегружая страницу веб-браузера. Можно также настроить автоматическое обновление таблицы событий, установив частоту обновления. По умолчанию автоматическое обновление отключено.

Чтобы включить автоматическое обновление,

Выберите частоту обновления в раскрывающемся списке в верхней правой части раздела **События**:

- **5 секунд**
- **15 секунд**
- **30 секунд**
- **1 минута**
- **5 минут**
- **15 минут**

Таблица событий обновляется автоматически.

Чтобы выключить автоматические обновление,

В раскрывающемся списке частоты обновления в верхней правой части раздела **События** выберите **Не обновлять**.

Получение статистики по событиям в таблице

Вы можете получить статистику по текущей выборке событий, отображаемой в таблице событий. Выборка событий зависит от параметров фильтрации.

Чтобы получить статистику:

в правом верхнем углу таблицы событий в раскрывающемся списке ••• выберите **Статистика** или в таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**.

Появится область деталей **Статистика** со списком параметров текущей выборки событий. Числа возле каждого параметра указывают количество событий в выборке, для которых задан этот параметр. Если параметр раскрыть, отображается его пять наиболее частых значений. С помощью поля **Поиск полей** можно найти нужные параметры.

В отказоустойчивой конфигурации для всех полей событий, которые содержат FQDN Ядра, в разделе **Статистика** будет отображаться не FQDN, а **core**.

В окне **Статистика** можно менять фильтр событий.

При использовании для фильтрации событий SQL-запросов с группировкой и агрегацией данных статистика недоступна.

Просмотр информации о корреляционном событии

Вы можете просматривать подробные сведения о корреляционном событии в окне **Информация о корреляционном событии**.

Чтобы просмотреть информацию о корреляционном событии:

1. В разделе **События** веб-интерфейса KUMA нажмите на корреляционное событие.

   Вы можете использовать фильтры для поиска корреляционных событий, присвоив значение `correlated` параметру `Type`.

   Откроется область деталей выбранного события.

2. Нажмите на кнопку **Подробные сведения**.

   Откроется окно корреляционного события. Название события отображается в левом верхнем углу окна.

Вы также можете перейти к окну корреляционного события из окна информации об алерте из раздела Связанные события. В этом случае вы можете вернуться к окну информации об алерте с помощью ссылки в верхней части окна. В других случаях KUMA не отображает ссылку на алерт.

В разделе **Информация о корреляционном событии** окна корреляционного события отображаются следующие данные:

- **Уровень важности корреляционного события** – важность корреляционного события.
- **Правило корреляции** – название правила корреляции, которое породило корреляционное событие. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.
- **Уровень важности правила корреляции** – важность правила корреляции, вызвавшего корреляционное событие.

- **Идентификатор правила корреляции** – идентификатор правила корреляции, которое породило корреляционное событие.

- **Тенант** – название тенанта, которому принадлежит корреляционное событие.

Раздел **Связанные события** окна корреляционного события содержит таблицу событий, относящихся к корреляционному событию. Это базовые события, в результате обработки которых было создано корреляционное событие. При выборе события в правой части окна веб-интерфейса открывается область деталей.

Ссылка **Найти в событиях** справа от заголовка раздела используется для расследования алерта.

Раздел **Связанные активы** окна корреляционного события содержит таблицу узлов, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием. При нажатии на название актива открывается окно **Информация об активе**.

Раздел **Связанные пользователи** окна корреляционного события содержит таблицу пользователей, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием.

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.
			Например:
			`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. Например: `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.
			Например:
			`enrich_table('Main/some-table', [DeviceProduct], 'value')`
			Ключевой может быть только один столбец таблицы, но ключ записи может быть составным.
			Например:
			`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. Например: • `enrich_dictionary('Main/some-dict', [SourceAddress]` • `enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress])` Вы можете посмотреть путь до словаря в разделе **Ресурсы** → **Словари**.

Примеры SQL-запросов с функцией enrich

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`.

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 одержит 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
```

Отслеживание маршрута событий

Чтобы выяснить, от какого подключения поступили события, вы можете использовать параметр **Отслеживать маршрут события**. Необходимость отслеживать маршрут события может возникать, когда несколько агентов отправляют события в один и тот же коллектор, например в крупной инфраструктуре, где агенты устанавливаются на выделенные серверы WEC и несколько агентов передают события в один и тот же коллектор. Данные о маршруте события могут быть полезны для диагностики проблем с поступлением событий.

Чтобы переключатель **Отслеживать маршрут события** стал доступен для использования, в агенте следует указать как минимум одну точку назначения с типом **internal**. Также для отслеживания маршрута событий необходимо, чтобы в коллекторе, который принимает события от агента, был указан коннектор типа **internal**. После настройки и сохранения агента информация о маршруте агента будет добавлена в поле расширенной схемы событий **S.KL_EventRoute**.

Поле **S.KL_EventRoute** появится только для новых событий, которые поступили в коллектор после включения параметра **Отслеживать маршрут события**. Другие сервисы, через которые проходит событие, включая коллектор, коррелятор (только правила корреляции типа simple), маршрутизатор, анализируют поле **S.KL_EventRoute**, и, если поле не пустое, при обработке события дописывают свои данные в поле.

Если событие проходит через несколько хостов от отправителя до агента, в поле **S.KL_EventRoute** сохраняется адрес последнего хоста, который установил соединение с агентом. Если между сервером-отправителем и агентом находится прокси-сервер, в поле будет зафиксирован адрес этого прокси-сервера, при этом на агенте не требуется отдельная настройка прокси-сервера. Коннекторы tcp/udp/http передают по протоколу **internal** в **S.KL_EventRoute** адрес хоста, от которого получено событие, а агенты WEC, WMI и ETW указывают имя хоста Windows-сервера, на котором они установлены.

Вы можете включить отслеживание маршрута события одним из следующих способов:

- Создать новый агент, в нем указать точку назначения типа **internal** и включить параметр **Отслеживать маршрут события**.

- В существующем агенте добавить вкладку с новым подключением и на этой вкладке указать точку назначения **internal**. После того как вы укажете точку назначения типа **internal**, параметр **Отслеживать маршрут события** станет доступен. Установите переключатель **Отслеживать маршрут события** в активное положение. После того как вы сохраните параметры агента, перезапустите агент, чтобы применить изменения. Отслеживание маршрута в этом случае действует только для той вкладки, где выбрана точка назначения **internal**, а не для всего агента.

- Отвязать автоматически созданный агент от коллектора, чтобы агент стал доступен для изменения параметров, или дублировать автоматически созданный агент и продолжить настройку параметров в дубликате агента. После того как вы укажете точку назначения типа **internal** в доступном для редактирования агенте, параметр **Отслеживать маршрут события** станет доступен. Установите переключатель **Отслеживать маршрут события** в активное положение. После того как вы сохраните параметры агента, перезапустите агент, чтобы применить изменения. Отслеживание маршрута в этом случае работает только для тех вкладок, где выбрана точка назначения **internal**, а не для всего агента.

В карточке события, в карточке алерта и карточке корреляционного события появится раздел **Журнал отслеживания событий**. В этом разделе отображается информация из поля **S.KL_EventRoute** в обработанном виде. Идентификаторы сервисов преобразованы в имена сервисов в виде ссылки. Если вы нажмете на имя сервиса, в браузере откроется новая вкладка с карточкой сервиса. Если вы измените название сервиса, имя сервиса также поменяется при отображении в карточке события, причем как для новых событий, так и для уже полученных и обработанных событий. Если вы удалите сервис в разделе **Активные сервисы**, в карточках событий в разделе **Журнал отслеживания событий** вместо гиперссылки будет отображаться **Удален**. Остальные данные о маршруте не будут удалены и продолжат отображаться, включая тип коннектора, FQDN, значение поля **SourceAddress** и другие параметры маршрута из поля **S.KL_EventRoute**. Чтобы просмотреть данные о маршруте в сыром виде, вы можете добавить в таблице событий столбец **S.KL_EventRoute**.

Использование информации о маршруте

Вы можете использовать функцию Extract from JSON или другие функции ClickHouse, чтобы получить нужные части маршрута для отладки. Подробнее о функциях см. в документации ClickHouse по ссылке: https://clickhouse.com/docs/ru/sql-reference/functions/json-functions#jsonextractstringjson-indices-or-keys

В таблице ниже приведены примеры запросов.

Пример запроса	Описание
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'version') as version FROM `events` Where Type !=4 ORDER BY Timestamp DESC LIMIT 25`	В результате этого запроса отобразятся события, для которых в столбце **version** отображается версия коллектора.
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') as connectorKind FROM `events` Where Type !=4 ORDER BY Timestamp DESC LIMIT 250`	В результате этого запроса отобразятся события, для которых в столбце **connectorKind** отображается тип коннектора.
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') as connectorKind FROM `events` Where Type !=4 and simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') != '"wec"' ORDER BY Timestamp DESC LIMIT 250`	В результате этого запроса отобразятся события, полученные от коннекторов с типом, отличным от wec.

Если вам нужна выборка по другому значению из поля **S.KL_EventRoute**, вы можете посмотреть наименование необходимого параметра в таблице событий в столбце **Raw**, чтобы использовать его в запросе.

Категоризация событий

Категоризация позволяет описать однотипные события из разных источников с помощью специальных тегов (категорий). Это упрощает задачу поиска событий, относящихся, например, к аутентификации пользователя или выполнению команды, а также помогает в написании корреляционной логики или отображении данных на панели мониторинга или в отчетах. С помощью набора ресурсов KUMA можно выполнить категоризацию некоторых типов событий для определенных типов источников событий.

Для категоризации событий используются следующие типы ресурсов KUMA:

- словарь с категориями событий;
- правила обогащения для дополнения событий информацией;
- нормализатор для создания поля расширенной схемы событий, используемого в правилах обогащения.

В процессе категоризации к событию могут быть добавлены следующие атрибуты:

- Object – объект.
- Action – действие.
- Result – результат.
- Threat – угроза.
- Source type – тип источника события.

Событию могут быть присвоены дополнительные атрибуты, которые сохраняются в поле SA.KL_EventCategory расширенной схемы событий.

Описания возможных значений атрибутов, используемых при категоризации событий, приведены в таблицах *Атрибут Object, Атрибут Action, Атрибут Result, Атрибут Threat, Атрибут Source type*.

Чтобы настроить категоризацию событий на коллекторе:

1. Импортируйте пакет [OOTB] Event Categorization из репозитория KUMA.
2. В коллекторе на шаге **Обогащение событий** примените правило обогащения событий.

   Вы можете применить правило обогащения как при создании нового коллектора, так и для уже существующего коллектора. Правило, которое необходимо применить, зависит от источника событий. Вы можете выбрать правило из таблицы *Правила категоризации по источнику событий*.

   > Категоризация событий работает только при использовании нормализаторов, поставляемых "Лабораторией Касперского".

3. В веб-интерфейс KUMA выберите раздел **Ресурсы** → **Активные сервисы**.

4. Установите флажок рядом с измененным коллектором и нажмите на кнопку **Обновить параметры**.

   Правило обогащения применено, категоризация событий выполняется.

Правила категоризации по источнику событий

Название системы	Название нормализатора	Название правила обогащения
Microsoft, журналы событий ОС	[OOTB] Microsoft Products for KUMA 3	[OOTB] Event categorization. Microsoft Products
Microsoft Sysmon	[OOTB] Microsoft Products for KUMA 3	[OOTB] Event categorization. Microsoft Products
Auditd	[OOTB] Linux auditd syslog for KUMA 3.2	[OOTB] Event categorization. Auditd
Kaspersky Security Center	[OOTB] KSC from SQL	[OOTB] Event categorization. Kaspersky Security Center
Kaspersky Security for Linux Mail Server	[OOTB] KLMS syslog CEF	[OOTB] Event categorization. Kaspersky Security for Linux Mail Server
Kaspersky IoT Secure Gateway	[OOTB] Kaspersky KISG syslog	[OOTB] Event categorization. Kaspersky IoT Secure Gateway
Kaspersky Container Security	[OOTB] Syslog-CEF	[OOTB] Event categorization. Kaspersky Container Security
Kaspersky Industrial CyberSecurity for Networks	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	[OOTB] Event categorization. Kaspersky Industrial CyberSecurity for Networks
Kaspersky Web Traffic Security	[OOTB] KWTS syslog CEF	[OOTB] Event categorization. Kaspersky Web Traffic Security
Kaspersky Mail Security Gateway	[OOTB] KSMG syslog CEF	[OOTB] Event categorization. Kaspersky Mail Security Gateway

Атрибут Object

Значение атрибута Object	Описание
account	Учетные записи
configuration	Параметры
connection	Сетевое соединение
container	Контейнеры
data	Данные или таблицы в БД
dns	DNS-запросы
email	Email
file	Файлы
group	Группы
host	Хост
http	WEB-запросы
image	DLL-библиотеки и драйвера
malware	Вредоносный объект
permission	Права и привилегии
process	Процесс
registry	Ключи и ветки реестра
service	Службы и демоны
task	Задачи
VM	Виртуальная машина

device	Токен, USB-устройство, подключаемое устройство
certificate	Сертификат

Атрибут Action

Значение атрибута Action	Описание
access	Запрос или предоставление доступа к объекту
add	Создание или добавление
authentication	Аутентификация
block	Блокировка, предотвращение
delete	Удаление
detect	Обнаружение или помещение в карантин
end	Конец процесса
info	Информационное событие об объекте
load	Загрузка объекта
modify	Изменение настроек или состояния объекта
read	Чтение
receive	Получение
request	Запрос
send	Отправка
start	Начало процесса
write	Запись

Атрибут Result

Значение атрибута Result	Описание
error	Ошибка
failure	Неуспешно
success	Успешно

Атрибут Threat

Значение атрибута Threat	Описание
malware	Вредоносный объект на файловой системе
vulnerability	Эксплуатации уязвимости
attack	Атака
ddos	Признаки DDoS-атаки
phishing	Признаки фишинга
c2	Command and Control
discovery	Разведка
policy violation	Нарушение политик безопасности
tools	Использование подозрительных инструментов
escalation	Повышение привилегий

Атрибут Source type

Значение атрибута Source type	Описание
application	События уровня приложений: входы, изменения конфигураций, ошибки и другое.
AV	События, поступающие от систем антивирусной защиты.

database	События, поступающие от баз данных, относящиеся к манипуляции с данными.
IDS	События, поступающие от анализаторов трафика и сетевых средств защиты.
network	События, содержащие сведения о сетевых соединениях, поступающие от межсетевых экранов или же события Netflow, Jflow и другое.
OS	События, поступающие от операционной системы, например, Windows, Linux, Cisco IOS, HP-UX и другое. Провайдером событий могут быть как штатные инструменты операционной системы, так и EDR.
vpn	События о VPN-сессиях.
web	События, поступающие от WEB-приложений и Proxy. События о HTTP-соединениях на уровне приложения.
container	События, содержащие сведения о работе контейнеров.

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** или прямо в карточке пользователя. После обновления до версии 4.0 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**, то хранилище и его пространства не отображаются в списке пространств набора.
- Если сервис хранилища был остановлен с помощью команды `systemctl stop kuma-<идентификатор хранилища>`, то хранилище и его пространства не отображаются в списке пространств набора.
- Если хранилище было запущено и далее удалено с помощью команды `uninstall`, то хранилище и его пространства продолжают отображаться в списке пространств набора.

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. Назначьте пользователям соответствующие роли.
2. Настройте наборы пространств.

   Вы можете создать, изменить, удалить набор пространств. По результатам этих действий формируются события аудита.
3. Регулируйте права доступа к набору пространств: можно 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.

Изменение 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

Переход на версию KUMA 4.0 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.

Изменение 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.

Панели мониторинга

В разделе **Панели мониторинга** вы можете контролировать состояние безопасности сети вашей организации.

Панель мониторинга представляет собой набор виджетов, которые отображают аналитику данных безопасности сети. Вы можете просмотреть данные только по тем тенантам, к которым у вас есть доступ.

Вы можете создавать панели мониторинга вручную или воспользоваться предустановленными панелями мониторинга. При необходимости вы можете изменить параметры виджетов в предустановленных панелях мониторинга. В качестве панели мониторинга по умолчанию используется предустановленная панель мониторинга Alerts Overview.

Создавать, изменять параметры и удалять панели мониторинга могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня и Аналитик первого уровня. Пользователи с учетными записями всех ролей могут просматривать панели мониторинга и назначать панели мониторинга по умолчанию. Если панель мониторинга установлена по умолчанию, она отображается для учетной записи при каждом переходе в раздел **Панели мониторинга**. Выбранная панель мониторинга по умолчанию сохраняется для текущей учетной записи пользователя.

Информация в разделе **Панели мониторинга** обновляется в соответствии с расписанием, заданным в параметрах панелей мониторинга. При необходимости вы можете обновить данные принудительно.

Для удобства представления данных на панелях мониторинга вы можете включить режим ТВ. В этом случае вы перейдете в режим полноэкранного просмотра панелей мониторинга в FullHD-разрешении. В режиме ТВ вы также можете настроить показ слайд-шоу для выбранных панелей мониторинга.

При необходимости вы можете просмотреть список всех доступных панелей мониторинга по тенантам, к которым они относятся, в левой части окна. С помощью кнопки **Скрыть панели** вы можете свернуть этот список, в этом случае отобразятся виджеты существующих панелей мониторинга. Вернуть список всех доступных панелей мониторинга по тенантам можно с помощью кнопки **Показать панели**.

Также в списке всех доступных панелей мониторинга по тенантам с помощью значка добавления + вы можете создавать папки для хранения панелей мониторинга в тенантах. Изменять параметры и удалять эти папки вы можете, нажав на значок меню ⋮ и выбрав соответствующее действие.

https://rutube.ru/video/304bc4fd81bae7219ade8c3a3d717213/

Создание панели мониторинга

Чтобы создать панель мониторинга:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панели мониторинга**.

2. Выполните одно из следующих действий:

   - Нажмите на значок меню (⋮) в правом верхнем углу окна и выберите **Создать панель**.

   - Нажмите на кнопку **Создать панель**, расположенную под списком всех панелей мониторинга.

   Откроется окно настройки параметров панели мониторинга.

3. В открывшемся окне укажите уникальное название панели мониторинга. Название должно содержать от 1 до 128 символов в кодировке Unicode и быть уникальным в рамках выбранного тенанта.

   Пользовательские панели мониторинга не могут иметь название предустановленных панелей мониторинга.

   При попытке создать панель мониторинга с названием предустановленной панели мониторинга или присвоить пользовательской панели мониторинга имя предустановленной панели мониторинга в тенанте Main вернется ошибка. В других тенантах, помимо тенанта Main, можно создать или дублировать пользовательскую панель мониторинга с именем предустановленной панели мониторинга.

4. В раскрывающемся списке **Тенант панели мониторинга** выберите тенант, которому будет принадлежать создаваемая панель мониторинга, или определенную папку в тенанте.

   Если у вас перед созданием панели мониторинга был открыт какой-либо набор графиков из одной из папок в тенанте, при создании панели мониторинга KUMA автоматически укажет этого тенанта. При необходимости, вы можете изменить тенанта.

5. В раскрывающемся списке **Собирать данные из тенантов** выберите один или несколько тенантов, данные из которых будут представлены в панели мониторинга.

6. При необходимости в раскрывающемся списке **Временной интервал** выберите период, по которому требуется аналитика, одним из следующих способов:

   - Если вы хотите указать **точную дату**, в календаре 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 выберете 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**.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите указать **пользовательский период**, задайте 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. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. 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 и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также 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.

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 в UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 сегодняшнего дня в UTC.

Время в Kaspersky SIEM хранится в UTC, но в веб-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 в UTC вчерашнего дня, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

7. При необходимости в раскрывающемся списке **Интервал обновления** выберите период обновления данных в виджетах панели мониторинга:

   - **Не обновлять** – данные в виджетах панели мониторинга не будут обновляться.
   - **1 минута**.
   - **5 минут**.
   - **15 минут**.
   - **1 час** (это значение выбрано по умолчанию).
   - **3 часа**.
   - **6 часов**.
   - **12 часов**.
   - **24 часа**.

8. При необходимости в раскрывающемся списке **Теги** выберите нужные теги для панели мониторинга.

9. При необходимости добавьте описание панели мониторинга.

10. С помощью переключателя **КИИ статус** включите отображение данных об активах, алертах и инцидентах, имеющих отношение к критической информационной инфраструктуре (КИИ). При этом такие панели мониторинга будут доступны для просмотра только пользователям, в параметрах которых установлен флажок **Доступ к объектам КИИ**.

    Если переключатель выключен, в виджетах панели мониторинга не будут отображаться данные об активах, алертах и инцидентах, относящихся к КИИ, даже если у пользователя есть доступ к объектам КИИ.

11. Нажмите **Применить**.

12. Нажмите на кнопку **Добавить виджет** и выберите требуемый виджет. В открывшемся окне настройте параметры выбранного виджета.

    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 стрелки (⤡), который появляется при наведении указателя мыши на правый нижний угол виджета.

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`).

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.

13. Нажмите **Создать**.

Панель мониторинга создана и отображается в разделе **Панели мониторинга** веб-интерфейса KUMA.

Вы также можете создать панель мониторинга на вкладке **Список** в разделе **Ресурсы**. Для этого необходимо нажать на кнопку **Добавить** и выбрать тип ресурса **Панель мониторинга**.

Выбор панели мониторинга

Чтобы выбрать панель мониторинга:

1. Раскройте список папок, в которых содержатся панели мониторинга, в верхнем левом углу окна **Панели мониторинга**.

   Папки с панелями мониторинга отображаются по их принадлежности тенантам.

2. Если вы хотите посмотреть панели мониторинга, которые вы создали, нажмите на кнопку **Созданные мною**.

   KUMA отобразит только созданные вами панели мониторинга макеты и только те папки, в которых находятся эти панели мониторинга. Папки, где находятся ваши панели мониторинга, могут быть созданы другими пользователями.

3. Выберите нужную папку и панель мониторинга в этой папке.

Выбранная панель мониторинга отобразится в окне **Панели мониторинга** веб-интерфейса KUMA.

Выбор панели мониторинга в качестве панели мониторинга по умолчанию

Чтобы выбрать панель мониторинга, которая будет отображаться по умолчанию:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. Раскройте список папок с панелями мониторинга в верхнем левом углу окна **Панели мониторинга**.
3. Найдите нужную панель мониторинга и нажмите на нее.
4. Выполните одно из следующих действий:
   - Нажмите на значок меню ⋮ рядом с панелью мониторинга в списке папок с панелями мониторинга, а затем в открывшемся списке команд выберите **Использовать по умолчанию**.
   - Нажмите на значок меню ⋮ в правом верхнем углу окна **Панели мониторинга** с открытой панелью мониторинга, а затем в открывшемся списке команд выберите **Установить по умолчанию**.

Выбранная панель мониторинга будет отмечена признаком **По умолчанию** и будет отображаться по умолчанию.

Изменение параметров панели мониторинга

Чтобы изменить параметры панели мониторинга:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. Раскройте список папок с панелями мониторинга в верхнем левом углу окна **Панели мониторинга**.
3. Найдите нужную панель мониторинга и нажмите на нее.
4. Нажмите на значок меню ⋮ рядом с панелью мониторинга в списке папок с панелями мониторинга, а затем в открывшемся списке команд выберите **Изменить**.
5. В открывшемся окне внесите изменения. Параметры, доступные для изменения, аналогичны параметрам, доступным при создании панели мониторинга.
6. Нажмите на кнопку **Сохранить**.

Параметры панели мониторинга будут изменены.

Если во время внесения изменений панель мониторинга была удалена или присвоена другому тенанту, при нажатии на кнопку **Сохранить** отобразится ошибка. Панель мониторинга не будет сохранена. Обновите страницу веб-интерфейса KUMA, чтобы в раскрывающемся списке просмотреть перечень доступных панелей мониторинга.

Удаление панели мониторинга

Чтобы удалить панель мониторинга:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. При необходимости нажмите на кнопку **Показать панели** в верхнем левом углу окна **Панели мониторинга** и раскройте список папок с панелями мониторинга.
3. Найдите панель мониторинга и нажмите на нее.
4. Выполните одно из следующих действий:
   - Нажмите на значок меню ⋮ рядом с панелью мониторинга в списке папок с панелями мониторинга, а затем в открывшемся списке команд выберите **Удалить**.
   - Нажмите на значок меню ⋮ в верхнем правом углу окна **Панели мониторинга** с открытой панелью мониторинга, а затем в открывшемся списке команд выберите **Удалить**.
5. Подтвердите удаление.

Панель мониторинга будет удалена.

Включение и выключение режима ТВ

Мы рекомендуем для отображения аналитики в режиме ТВ создать отдельного пользователя с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. В правом верхнем углу нажмите на кнопку **Режим ТВ**.
3. В открывшемся окне переведите переключатель **Режим ТВ** в положение **Включено**.
4. Если вы хотите настроить показ панелей мониторинга в режиме слайд-шоу, выполните следующие действия:
   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.
   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение панелей мониторинга.
   c. В блоке **Очередь** выберите панели мониторинга для просмотра и нажмите **Добавить в очередь**. Если панели мониторинга не выбраны, в режиме слайд-шоу будут по очереди отображаться все панели мониторинга, доступные пользователю.

d. При необходимости, удалите панель мониторинга. Для этого необходимо с помощью флажка выделить панель мониторинга в очереди и нажать **Удалить**.

e. Если требуется, измените порядок показа панелей мониторинга, перетаскивая их с помощью зажатой правой клавиши мыши.

5. Нажмите на кнопку **Сохранить**.

Режим ТВ будет включен.

Чтобы выключить режим ТВ,

нажмите на кнопку **Стоп** в правом верхнем углу окна, где ведется показ панелей мониторинга.

Режим ТВ будет выключен. В левой части экрана отобразится панель с разделами веб-интерфейса KUMA.

Если в выбранные для слайд-шоу панели мониторинга вносятся изменения, эти изменения будут автоматически отображаться в запущенных сессиях слайд-шоу.

Определение периода без изменения параметров панели мониторинга

При просмотре панели мониторинга KUMA отображается период, который указан в параметрах панели мониторинга. Если вам требуется посмотреть данные за другой период, вы можете установить нужный вам период, не изменяя параметры панели мониторинга.

Чтобы изменить период в панели мониторинга:

1. В разделе **Панели мониторинга** веб-интерфейса KUMA выберите панель мониторинга для просмотра.

   Выбранная панель мониторинга отобразится в окне **Панели мониторинга**. При открытии панель мониторинга сформирована в соответствии с последним обновлением данных по расписанию.

2. В раскрывающемся списке **Период**, который находится над панелью мониторинга, выберите интересующий вас календарный или относительный период.

3. Если вы выбрали точный календарный период, нажмите на кнопку **Применить**.

   Данные на панели мониторинга будут обновлены.

При изменении периода в панели мониторинга нужно учитывать следующее:

- Период, который вы устанавливаете описанным выше образом, не сохраняется в параметрах панели мониторинга. Если вы обновите страницу браузера или закроете и повторно откроете панель мониторинга, отобразится период, указанный в параметрах панели мониторинга.

- В виджетах в панели мониторинга учитывается установленный период. Если вы укажете другой период в панели мониторинга, данные изменятся только у виджетов, у которых для параметра **Период** выбрано значение **Как на панели мониторинга**.

- Интерактивность данных в режиме ТВ не предусмотрена, поэтому раскрывающийся список **Период** не отображается и задать новый период невозможно.

Предустановленные панели мониторинга

KUMA поставляется с набором предустановленных панелей мониторинга. По умолчанию для предустановленных панелей мониторинга указан период обновления **Никогда**. Вы можете изменить эти панели мониторинга при необходимости.

Название панели мониторинга	Описание виджетов в составе панелей мониторинга
Alerts Overview (Обзор алертов)	• Active alerts (Активные алерты) – количество незакрытых алертов. • Unassigned alerts (Неназначенные алерты) – количество алертов со статусом **Новый**. • Latest alerts (Последние алерты) – таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в панели мониторинга тенантам. • Alerts distribution (Распределение алертов) – количество алертов, созданных в течение указанного для виджета периода. • Alerts by priority (Алерты по уровню важности) – количество незакрытых алертов, сгруппированных по уровню важности. • Alerts by assignee (Алерты по исполнителю) – количество алертов со статусом **Назначен**. Сгруппированы по имени учетной записи. • Alerts by status (Алерты по статусу) – количество алертов, имеющих статус **Новый**, **Открыт**, **Назначен** или **Эскалирован**. Сгруппированы по статусу. • Affected users in alerts (Затронутые пользователи) – количество пользователей, связанных с алертами, имеющими статус **Новый**, **Назначен** или **Эскалирован**. Сгруппированы по имени учетной записи. • Affected assets (Затронутые активы) – таблица с информацией об уровне важности активов и количестве незакрытых алертов, с которыми они связаны. • Affected assets categories (Затронутые категории активов) – категории активов, привязанных к незакрытым алертам. • Top event source by alerts number (Топ источников событий по количеству алертов) – количество алертов со статусом **Новый**, **Назначен** или **Эскалирован**, сгруппированных по источнику алерта (поле события DeviceProduct). На виджете отображается не более 10 источников событий. • Alerts by rule (Количество алертов по правилу) – количество алертов со статусом **Новый**, **Назначен** или **Эскалирован**, сгруппированных по правилам корреляции.
Incidents Overview (Обзор инцидентов)	• Active incidents (Активные инциденты) – количество незакрытых инцидентов. • Unassigned Incidents (Неназначенные инциденты) – количество инцидентов со статусом **Открыт**. • Latest Incidents (Последние инциденты) – таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в панели мониторинга тенантам. • Incidents distribution (Распределение инцидентов) – количество инцидентов, созданных в течение указанного для виджета периода. • Incidents by priority (Инциденты по уровню важности) – количество незакрытых инцидентов, сгруппированных по уровню важности. • Incidents by assignee (Инциденты по исполнителю) – количество инцидентов со статусом **Назначен**. Сгруппированы по имени учетной записи пользователя. • Incidents by status (Инциденты по статусам) – количество инцидентов, сгруппированных по статусу. • Affected assets in incidents (Активы в инцидентах) – количество активов, связанных с незакрытыми инцидентами. • Affected users in incidents (Пользователи в инцидентах) – пользователи, связанные с незакрытыми инцидентами. • Affected asset categories in incidents (Категории активов в инцидентах) – категории активов, связанных с незакрытыми инцидентами. • Active incidents by tenant (Инциденты по тенантам) – количество инцидентов всех статусов, сгруппированных по тенантам.
Network Overview (Обзор сетевой активности)	• Netflow top internal IPs (Топ внутренних 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.
[OOTB] KATA & EDR	• KATA. Top-10 detections by type – визуализирует 10 самых распространенных типов событий, выявленных системой KATA. • KATA. Top-10 detections by file type – визуализирует 10 самых распространенных типов файлов, выявленных системой KATA. • KATA. Top-10 user names in detections – визуализирует 10 самых распространенных имен пользователей, выявленных системой KATA. • KATA. Top-10 IDS detections – визуализирует 10 самых распространенных угроз, выявленных модулем IDS системы KATA. • KATA. Top-10 URL detections – визуализирует 10 самых распространенных подозрительных URL-адресов, выявленных системой KATA. • KATA. Top-10 AV detections – визуализирует 10 самых распространенных угроз, выявленных модулем антивируса системы KATA. • EDR. Top-10 MITRE technique detections – визуализирует 10 самых распространенных техник матрицы MITRE ATT&CK, выявленных системой EDR. • EDR. Top-10 MITRE tactic detections – визуализирует 10 самых распространенных тактик матрицы MITRE ATT&CK, выявленных системой EDR.

Название панели мониторинга	Описание виджетов в составе панелей мониторинга
[OOTB] KSC	• KSC. Top-10 users with the most KAV alerts – визуализирует 10 самых распространенных имен пользователей, присутствующих в событиях, связанных с выявлением вредоносного программного обеспечения, сведения о которых содержатся в системе KSC. • KSC. Top-10 most common threats – визуализирует 10 самых распространенных типов вредоносного программного обеспечения, сведения о которых содержатся в системе KSC. • KSC. Number of devices that received AV database updates – визуализирует количество устройств, на которых были установлены обновления антивирусных баз данных, сведения о которых содержатся в системе KSC. • KSC. Number of devices on which the virus was found – визуализирует количество устройств, на которых было выявлено вредоносное программное обеспечение, сведения о которых содержатся в системе KSC. • KSC. Malware detections by hour – визуализирует распределение по часам количества вредоносного программного обеспечения, сведения о которых содержатся в системе KSC.
[OOTB] KSMG	• KSMG. Top-10 senders of blocked emails – визуализирует 10 самых распространенных отправителей писем, заблокированных системой KSMG. • KSMG. Top-10 events by action – визуализирует 10 самых распространенных действий, выполненных системой KSMG. • KSMG. Top-10 events by outcome – визуализирует 10 самых распространенных результатов действий, выполненных системой KSMG. • KSMG. Blocked emails by hour – визуализирует распределение по часам количества писем, заблокированных системой KSMG.
[OOTB] KWTS	• KWTS. Top-10 IP addresses with the most blocked web traffic – визуализирует 10 самых распространенных IP-адресов, трафик с которых был заблокирован системой KWTS. • KWTS. Top-10 IP addresses with the most allowed web traffic – визуализирует 10 самых распространенных IP-адресов, трафик с которых был разрешен системой KWTS. • KWTS. Top 10 requests by client application – визуализирует 10 самых распространенных приложений, использовавшихся для доступа к сетевым ресурсам, выявленных системой KWTS. • KWTS. Top-10 blocked URLs – визуализирует 10 самых распространенных URL-адресов, трафик с которых был разрешен системой KWTS. • KWTS. System action types – визуализирует 10 самых распространенных действий, выполненных системой KWTS. • KWTS. Top-10 users with the most allowed web traffic – визуализирует 10 самых распространенных имен пользователей, трафик которых был разрешен системой KWTS.
[OOTB] KSMG files and hashes*	• KSMG. Top-5 blocked hashes - визуализирует 5 самых распространенных хешей файлов в письмах, заблокированных системой KSMG. • KSMG. Top-5 net-transferred hashes - визуализирует 5 самых распространенных "чистых" хешей файлов в письмах, отслеженных системой KSMG. • KSMG. Top-5 clean file names - визуализирует 5 самых распространенных "чистых" имен файлов в письмах, отслеженных системой KSMG. • KSMG. Top-5 blocked files - визуализирует 5 самых распространенных имен файлов в письмах, заблокированных системой KSMG.
[OOTB] KSMG rules and URLs*	• KSMG. Top-5 rules - визуализирует 5 самых распространенных сработанных правил системы KSMG. • KSMG. Top-5 URLs - визуализирует 5 самых распространенных доменов из ссылок в письмах, отслеженных системой KSMG.
[OOTB] KSMG results*	• KSMG. All results in the last 24 hours - визуализирует распределение по часам действий, выполненных системой KSMG за сутки. • KSMG. Top-5 results - визуализирует 5 самых распространенных действий, выполненных системой KSMG.
[OOTB] KSMG e-mail subjects and accounts*	• KSMG. Top-5 e-mail subjects - визуализирует 5 самых распространенных тем писем, отслеженных системой KSMG. • KSMG. Top-5 source accounts - визуализирует 5 самых распространенных аккаунтов отправителей писем, отслеженных системой KSMG. • KSMG. Top-5 destination accounts - визуализирует 5 самых распространенных аккаунтов получателей писем, отслеженных системой KSMG.

*Панели мониторинга доступны начиная с KUMA 3.4.1. Виджеты будут корректно отображать информацию при использовании нормализатора [OOTB] KSMG 2.1+ syslog CEF.

Универсальность панелей мониторинга

Панель мониторинга в KUMA считается универсальной, если создается в тенанте Shared. Панели мониторинга, созданные в других тенантах, являются неуниверсальными.

Универсальная панель мониторинга

Универсальная панель мониторинга имеет следующие свойства:

- Универсальная панель мониторинга доступна для просмотра всем ролям пользователей и во всех тенантах.
- Данные для тенантов отображаются в соответствии с общим фильтром тенантов.
- Данные в виджетах по событиям из базы данных получаются в соответствии с настроенными для пользователя параметрами пространств.

Для работы с универсальной панелью мониторинга 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.
- Для просмотра списка универсальных панелей мониторинга нужна роль Чтение общих ресурсов. При наличии такой роли пользователь получает доступ на чтение всех общих ресурсов в разделе **Ресурсы**.

  Если вам назначена роль с доступом к универсальным панелям мониторинга, вы можете просмотреть список универсальных панелей мониторинга в разделах **Панели мониторинга** и **Ресурсы**, но доступа к другим ресурсам тенанта Shared у вас не будет.

Для просмотра актуальных данных в универсальных панелях мониторинга нужно подписаться на изменения таких панелей. Подписку можно оформить на все панели мониторинга в тенанте Shared, даже на созданные вами панели мониторинга.

Чтобы подписаться на панель мониторинга в тенанте Shared:

1. В разделе **Панели мониторинга** в списке панелей мониторинга выберите и откройте панель мониторинга в тенанте Shared.
2. Нажмите на значок меню ⋮ в правом верхнем углу открытой панели мониторинга.
3. В открывшемся списке команд выберите **Подписаться на изменения**.

   При необходимости вы можете отказаться от подписки, выбрав **Отписаться от изменений** в списке действий.

Если роль пользователя предполагает работу с ресурсами КИИ, то данные на панели мониторинга будут отображаться с учетом признака КИИ.

Неуниверсальная панель мониторинга

Неуниверсальная панель мониторинга создается в любом тенанте KUMA, кроме Shared. Такие панели мониторинга имеют следующие свойства:

- Панели мониторинга доступны для просмотра пользователям, у которых есть доступ к тенанту, в котором создана панель мониторинга.
- Доступ к данным виджетов в панели мониторинга есть только у пользователей, у которых есть доступ к тенанту, в котором создана панель мониторинга.
- Если панели мониторинга присвоен признак КИИ, данные на панели мониторинга будут доступны при наличии у пользователя прав на доступ к КИИ.

Экспорт панелей мониторинга

Чтобы экспортировать панель мониторинга:

1. В разделе **Ресурсы** перейдите на вкладку **Список**.

   Откроется окно со списком всех ресурсов, доступных вам в KUMA.

   При необходимости вы можете настроить отображение ресурсов на существующих панелях мониторинга, выбрав **Панель мониторинга** в столбце **Тип ресурса**.

2. С помощью флажка выберите панель мониторинга для экспорта.
3. Нажмите на кнопку **Экспортировать**, расположенную над таблицей со списком ресурсов.
4. В открывшейся боковой панели выполните следующие действия:

   a. Укажите пароль к файлу с экспортируемыми ресурсами. Пароль должен соответствовать следующим требованиям:

      - длина минимум 16 символов;
      - как минимум один символ в нижнем регистре;
      - как минимум один символ в верхнем регистре;
      - как минимум одна цифра;
      - как минимум один специальный символ.

   b. В раскрывающемся списке **Тенант** выберите тенант, из которого вы хотите экспортировать выбранные ресурсы.

   c. С помощью установки 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**.

   Файл для экспорта сохраняется в папку загрузки, настроенную в вашем браузере.

При экспорте панелей мониторинга необходимо учитывать следующее:

- Панели мониторинга экспортируются без информации о тенантах, хранилищах и пространствах, поскольку эти параметры устанавливаются отдельно для каждого развертывания KUMA.
- Виджеты панелей мониторинга также экспортируются без информации о тенантах, хранилищах и пространствах.
- Параметры SQL-функций enrich и lookup в запросах виджетов экспортируются без изменений. При необходимости вы можете их изменить в соответствии со своими требованиями после экспорта ресурсов.
- Ссылки на активные листы и таблицы не экспортируются. При необходимости вы можете настроить эти виджеты после экспорта ресурсов.

Импорт панелей мониторинга

Чтобы импортировать панель мониторинга:

1. В разделе **Ресурсы** перейдите на вкладку **Список**.

   Откроется окно со списком всех ресурсов, доступных вам в KUMA.

   При необходимости вы можете настроить отображение ресурсов на существующих панелях мониторинга, выбрав **Панель мониторинга** в столбце **Тип ресурса**.

2. С помощью флажка выберите панель мониторинга 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 панель мониторинга.
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 панелей мониторинга необходимо учитывать следующее:

- Если вы импортируете панель мониторинга в выбранный тенант и exportID импортируемой панели мониторинга совпадает с exportID панели мониторинга, которая уже есть в тенанте, вернется сообщение о конфликте и варианты разрешения конфликта. Вам нужно выбрать одну из следующих опций:

  - **Пропустить**.

    Если вы выберете **Пропустить**, будут импортированы все выбранные для импорта ресурсы, кроме конфликтного.

  - **Заменить**.

    Если вы выберете **Заменить**, панель мониторинга будет импортирована и данные будут записаны поверх.

  Если вы хотите посмотреть разницу между панелями мониторинга с одинаковым exportID, вы можете нажать **Пропустить**, а затем импортировать панель мониторинга в другой тенант и сравнивать панели мониторинга в разных тенантах.

- Если название импортируемой панели мониторинга совпадает с названием панели мониторинга, которая уже есть в тенанте, панель мониторинга будет импортирована и к названию будет добавлена дата и время импорта. Например, Alerts Overview-2025-11-26 12:52:59.

- Если панель мониторинга содержит виджет **События**, мы рекомендуем импортировать панель мониторинга в тенант **Shared**. Такая панель мониторинга становится универсальной.

- Для импорта панели мониторинга в тенант **Shared** требуется роль Редактирование общих ресурсов. Для просмотра такой панели мониторинга следует подписаться на панель мониторинга.

- Если панель мониторинга импортируется в тенант **Shared**, в панели мониторинга автоматически указываются все хранилища, поскольку доступ к ним определяется в параметрах пользователя.

- Если панель мониторинга импортируется в любой тенант, кроме **Shared**, то тенант импортируемой панели мониторинга указывается в качестве тенанта ресурса, тенанта источника данных и хранилища. После импорта ресурсов необходимо указать пространства для виджетов с событиями и при необходимости расширить список тенантов.

- Параметры SQL-функций enrich и lookup в запросах виджетов импортируются без изменений. При необходимости вы можете их изменить в соответствии со своими требованиями после импорта ресурсов.

- Ссылки на активные листы и таблицы не импортируются. При необходимости вы можете настроить эти виджеты после импорта ресурсов.

- Если панель мониторинга содержит виджет **Активные листы** или **Контекстные таблицы**, мы рекомендуем дублировать такие панели мониторинга и изменять параметры дубликатов, адаптируя к своей инфраструктуре – указывать коррелятор, выбирать активные листы и контекстные таблицы.

Отчеты

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://rutube.ru/video/3aadb7010e5aaffca1a529456a8a35e9/

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, сформированные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. В таблице представлена следующая информация:

- **Название** – название 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.

  > 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 ⌄ 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 веб-интерфейсе выполните одно из следующих действий:
   - Откройте раздел **Отчеты** → **Шаблоны** и в панели инструментов или в меню ⋮ нажмите **Создать**.
   - Откройте раздел **Ресурсы** → **Список**, в панели инструментов или в меню ⋮ нажмите **Создать** и выберите **Шаблон отчетов**.

Справа откроется панель создания шаблона отчета.

2. В поле **Название шаблона** укажите название шаблона отчета. Название должно содержать от 1 до 128 символов в кодировке Unicode и быть уникальным в рамках выбранного тенанта.

> Названия создаваемых шаблонов отчетов не могут совпадать с названиями предустановленных шаблонов отчетов в тенанте Main.

> При попытке создать шаблон отчета с названием предустановленного шаблона отчетов или присвоить шаблону отчета название предустановленного шаблона отчета в тенанте Main вернется ошибка. В других тенантах можно создать или дублировать шаблон отчета с именем предустановленного шаблона отчета. Мы рекомендуем использовать уникальные имена для создаваемых шаблонов отчетов.

3. В раскрывающемся списке **Тенант шаблона** выберите тенант, которому будет принадлежать создаваемый шаблон отчета.

4. В раскрывающемся списке **Собирать данные от тенантов** выберите один или несколько тенантов, на основе данных которых будут формироваться отчеты.

5. При необходимости в раскрывающемся списке **Временной интервал** выберите период, по которому требуется аналитика, одним из следующих способов:

   - Если вы хотите указать **точную дату**, в календаре 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 выберете 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**.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите указать **пользовательский период**, задайте 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. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. 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 и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также 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.

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 Kaspersky SIEM хранится в UTC, но в веб-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 в UTC вчерашнего дня, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

6. При необходимости в поле **Срок хранения** укажите, в течение какого времени будут храниться сформированные по этому шаблону отчеты.

   По умолчанию указано 3 месяца.

7. При необходимости в раскрывающемся списке **Теги** выберите теги для шаблона отчета.

8. При необходимости добавьте описание шаблона отчета.

9. 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.

10. Нажмите **Сохранить**.

    Откроется окно изменения отчета.

11. При необходимости добавьте логотип шаблона отчета, перетащив изображение в поле или нажав на ссылку **Загрузите файл**. Изображение должно быть в формате JPG, PNG или GIF. Максимальный размер изображения – 3 МБ.

    Добавленный логотип будет отображаться в отчете вместо логотипа решения.

12. Нажмите на кнопку **Добавить виджет** и выберите нужный виджет. В открывшемся окне настройте параметры выбранного виджета.

Вы можете добавить несколько виджетов. Виджеты можно перетаскивать с помощью значка перетаскивания (⠿), расположенного рядом с левым верхним углом виджета. Если вы хотите изменить размер виджета, вы можете используйте значок растяжения (⤡), который появляется при наведении курсора мыши на правый нижний угол виджета.

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`).

Нажав на значок меню ⋮ в правом верхнем углу виджета, вы можете изменять параметры виджетов, копировать и удалять виджеты.

13. Нажмите **Создать**.

Новый шаблон отчета будет создан. Вы можете сформировать этот отчет вручную или настроить расписание для автоматического формирования отчетов.

Настройка расписания отчетов

Вы можете настроить расписание, по которому отчеты будут автоматически отправляться на указанные адреса электронной почты.

Если в отправляемом отчете присутствуют только виджеты с ошибками, отчет не будет отправлен. Если в отчете присутствует хотя бы один виджет без ошибок, отчет будет отправлен.

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 **Отправлять 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 **Параметры 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 для направления отчета. Для выбора доступны следующие форматы: HTML, PDF, 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 получатели не являются пользователями KUMA, переход по ссылкам будет доступен, но авторизоваться в KUMA получатели не смогут, поэтому им будут доступны только вложения.

Мы рекомендуем 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 авторизацией в KUMA, без ограничений по ролям или тенантам.

d. Нажмите **Добавить**.

6. Нажмите **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**.

3. Внесите необходимые изменения:

   - Измените название шаблона отчета. Оно должно быть уникальным в рамках выбранного тенанта.

     Пользовательские шаблоны отчетов не могут иметь название предустановленных шаблонов отчетов.

     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.
   - Измените список тенантов, которые передают данные для отчета.
   - Нажмите на кнопку **Параметры** для изменения временного периода для получения аналитических данных, срок хранения, теги и описание 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 **Сохранить**.

Шаблон отчета изменен и отображается на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список** веб-интерфейса KUMA.

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:

   - Временной интервал формирования отчета.

   - Срок хранения отчета.

   - Теги шаблона отчета.

   - Описание шаблона отчета.

   - Формирование данных в отчете с учетом КИИ.

7. Нажмите **Сохранить**.

Копия шаблона отчета создана и отображается на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список** веб-интерфейса KUMA.

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 раздел **Ресурсы** → **Список**.

   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. В панели инструментов или в меню ⋮ нажмите **Экспортировать**.
3. В открывшейся боковой панели выполните следующие действия:
   a. Укажите пароль к файлу с экспортируемыми ресурсами. Пароль должен соответствовать следующим требованиям:
      - длина минимум 16 символов;
      - как минимум один символ в нижнем регистре;
      - как минимум один символ в верхнем регистре;
      - как минимум одна цифра;
      - как минимум 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.

4. Нажмите на кнопку **Экспортировать**.

При экспорте шаблонов отчета необходимо учитывать следующее:

- Шаблоны отчетов экспортируются без информации о тенантах, хранилищах и пространствах, поскольку эти параметры устанавливаются отдельно для каждого развертывания KUMA.
- Виджеты шаблона отчета также экспортируются без информации о тенантах, хранилищах и пространствах.
- Если перед экспортом вы удалили предустановленный шаблон отчетов и создали пользовательский шаблон отчетов с именем предустановленного, то при экспорте к названию шаблона отчетов будет добавлена дата и время экспорта. Например, Incidents Overview-2025-11-26 12:52:59.

Чтобы импортировать шаблон отчета:

1. Откройте веб-интерфейс KUMA и перейдите в раздел **Ресурсы** → **Список**.

   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. В панели инструментов или в меню ⋮ нажмите **Импортировать**.
3. В открывшейся боковой панели в раскрывающемся списке **Тенант** выберите тенант, в который вы хотите импортировать шаблон отчета.
4. Выберите источник импорта: **Файл** или **Репозиторий**.
5. 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.

6. Нажмите на кнопку **Импортировать**.
7. При необходимости устраните конфликты между импортированными из файла и существующими ресурсами.

При импорте шаблона отчета необходимо учитывать следующее:

- Если вы импортируете шаблон отчетов и exportID импортируемого шаблона отчетов совпадает с exportID шаблона отчетов, который уже есть в тенанте, вернется сообщение о конфликте и варианты разрешения конфликта. Вам нужно выбрать одну из следующих опций:

  - **Пропустить**.

    Если вы выберете **Пропустить**, будут импортированы все выбранные для импорта ресурсы, кроме конфликтного.

  - **Заменить**.

    Если вы выберете **Заменить**, шаблон отчетов будет импортирован и данные будут записаны поверх.

  Если вы хотите посмотреть разницу между шаблонами отчетов с одинаковым exportID, вы можете нажать **Пропустить**, а затем импортировать шаблон отчетов в другой тенант и сравнивать шаблоны отчетов в разных тенантах.

- Если название импортируемого шаблона отчетов совпадает с названием шаблона отчетов, который уже есть в тенанте, шаблон отчетов будет импортирован и к названию будет добавлена дата и время импорта. Например, Incidents Overview-2025-11-26 12:52:59.

- 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, где представлена следующая информация:

- **Название** – название 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 окно с виджетами, отображающими аналитику отчетов. Если виджет отображает данные о событиях, алертах, инцидентах, активных листах и контекстных таблицах 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 один из следующих вариантов 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** выполните следующие действия:

      - 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.

Если отчет в формате CSV или Excel содержит виджеты с одинаковыми названиями, файлы виджетов будут автоматически переименованы с добавлением числового суффикса в имени файла. Так как переименование происходит автоматически, то при сохранении одного отчета в разные форматы суффиксы переименованных файлов одного и того же виджета в разных форматах могут не совпадать, например, файл `widget(2)` в одном формате не обязательно соответствует файлу `widget(2)` в другом формате. Для удобства рекомендуется называть виджеты уникальными именами вне зависимости от формата отчета.

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 отчет.
3. Нажмите на кнопку **Удалить**, расположенную над таблицей.

   Откроется окно подтверждения.
4. Нажмите **Удалить**.

Выбранный отчет удален.

Виджеты

С помощью виджетов вы можете осуществлять мониторинг работы решения. Виджеты организованы в группы, каждая из которых связана с типом аналитики, которую она предоставляет. В KUMA доступны следующие группы 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 аналитики алертов.

  В группу входят следующие виджеты:

  - **Активные алерты** – количество незакрытых алертов.
  - **Активные алерты по тенантам** – количество незакрытых алертов для каждого тенанта.
  - **Алерты по тенантам** – количество алертов всех статусов для каждого тенанта.
  - **Неназначенные алерты** – количество алертов со статусом **Новый**.
  - **Алерты по исполнителю** – количество алертов со статусом **Назначен**, сгруппированных по имени учетной записи.
  - **Алерты по статусу** – количество алертов со статусом **Новый**, **Открыт**, **Назначен** или **Эскалирован**, сгруппированных по статусу.
  - **Алерты по уровню важности** – количество незакрытых алертов, сгруппированных по уровню важности.
  - **Алерты по правилу корреляции** – количество незакрытых алертов, сгруппированных по правилам корреляции.
  - **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.
- **Активы** – группа для аналитики активов из обработанных событий. В эту группу входят следующие виджеты:

  - **Затронутые активы** – таблица с информацией об уровне важности активов и количестве незакрытых алертов, с которыми они связаны.
  - **Категории затронутых активов** – категории активов, привязанных к незакрытым алертам.
  - **Количество активов** – количество активов, добавленных в KUMA.

- **Активы в инцидентах по тенантам** – количество активов, связанных с незакрытыми инцидентами. Сгруппированы по тенантам.
- **Активы в алертах по тенантам** – количество активов, связанных с незакрытыми алертами, Сгруппированы по тенантам.

- Инциденты – группа для аналитики инцидентов.

  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 исполнителю** – количество инцидентов со статусом **Назначен**, сгруппированных по имени учетной записи пользователя.
  - **Инциденты по статусам** – количество инцидентов, сгруппированных по статусу.
  - **Инциденты по уровню важности** – количество незакрытых инцидентов, сгруппированных по уровню важности.
  - **Активные инциденты по тенантам** – количество незакрытых инцидентов, сгруппированных по тенантам, доступным для учетной записи пользователя.
  - **Все инциденты** – количество инцидентов всех статусов.
  - **Все инциденты по тенантам** – количество инцидентов всех статусов, сгруппированных по тенантам.
  - **Активы в инцидентах** – количество активов, связанных с незакрытыми инцидентами.
  - **Категории активов в инцидентах** – категории активов, связанных с незакрытыми инцидентами.
  - **Пользователи в инцидентах** – пользователи, связанные с инцидентами.
  - **Последние инциденты** – таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.

- **Источники событий** – группа для аналитики источников событий. В группу входят следующие виджеты:
  - **Топ источников событий (значение в поле DeviceProduct) по количеству базовых событий, собранных в корреляционных событиях** – количество базовых событий, собранных в корреляционных событиях и сгруппированных по источникам данных, указанным в поле DeviceProduct.
  - **Топ источников событий (значение в поле DeviceProduct) по условному рейтингу** – соотношение между числом базовых событий в корреляционных событиях и общим числом базовых событий, сгруппированных по источникам данных, указанным в поле DeviceProduct.

    В ряде случаев количество корреляционных событий, 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:
  - **Пользователи в алертах** – количество учетных записей, связанных с незакрытыми алертами.
  - **Количество пользователей AD** – количество учетных записей в Active Directory, полученных по LDAP в течение указанного для виджета периода.
- Изображение – виджет для отображения загруженного изображения на панели мониторинга или в отчете.
- Текст – виджет для отображения произвольного текста на панели мониторинга или в отчете.

В таблице событий, в области деталей событий, в окне алертов, а также в виджетах в качестве значений полей `SourceAssetID`, `DestinationAssetID`, `DeviceAssetID`, `SourceAccountID`, `DestinationAccountID` и `ServiceID` вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Основные принципы работы с виджетами

Принцип отображения данных на виджете зависит от типа графика. В KUMA доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).
- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).

- Линейная диаграмма.
- Сложенная столбчатая диаграмма.
- Спидометр.

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 веб-интерфейса KUMA.

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 для виджета вы включили параметр **Показывать данные за предыдущий период**, и данные на виджете отображаются за относительный период, во всплывающей подсказке также будет отображаться предыдущий период. Предыдущий период рассчитывается относительно текущего периода как значения начала и конца текущего периода минус длительность 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). Название скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

Данные на виджете отображаются за выбранный в параметрах виджета или макета период только для тенантов, которые были выбраны 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. Щелкнув левой кнопкой мыши по категории в легенде, вы можете перейти в раздел веб-интерфейса KUMA с соответствующими данными. Данные в этом 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 запрос возвращает данные, которые разбиваются на большое количество секторов, то для оптимизации отображения виджета добавляется сектор **Другое**. Вы можете уменьшить размер сектора **Другое**, составив более детализированный запрос. Для детализации запроса вы можете использовать функции `LIMIT` и `WHERE`.

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**.
  Для настройки отображения трендов требуется включить переключатель **Показывать данные за предыдущий период**, а затем на вкладке **Внешний вид** выбрать тренд. Если значение в процентах нельзя подсчитать 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. Щелкнув левой кнопкой мыши по категории в легенде, вы можете перейти в раздел веб-интерфейса KUMA с соответствующими данными. Данные в этом 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 запрос возвращает данные, которые разбиваются на большое количество столбцов, то для оптимизации отображения виджета добавляется столбец **Другое**. Вы можете уменьшить размер столбца **Другое**, составив более детализированный запрос. Для детализации запроса вы можете использовать функции `LIMIT` и `WHERE`.

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. Щелкнув левой кнопкой мыши по категории в легенде, вы можете перейти в раздел веб-интерфейса KUMA с соответствующими данными. Данные в этом 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, хосты. Градиентная заливка к такому графику не применяется.

Пример запроса для отображения линейной диаграммы с несколькими линиями

```
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. Щелкнув левой кнопкой мыши по категории в легенде, вы можете перейти в раздел веб-интерфейса KUMA с соответствующими данными. Данные в этом 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 курсорамыши на области столбца отображается подсказка со значением и описанием значения. Вы можете перейти в раздел веб-интерфейса KUMA с соответствующими данными, щелкнув левой кнопкой мыши по категории в легенде.

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 в 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 в 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. График **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 графика **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 показыть 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 графика **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 на панели мониторинга в процессе создания или изменения панели мониторинга.

Чтобы создать виджет:

1. Создайте панель мониторинга или перейдите в режим изменения выбранной панели мониторинга.
2. Нажмите на кнопку **Добавить виджет**.
3. В раскрывшемся списке выберите тип виджета.

   Отобразится окно параметров виджета.
4. Задайте параметры виджета.
5. Если вы хотите просмотреть, как будут отображаться данные на виджете, нажмите на кнопку **Предварительный просмотр**.
6. Нажмите на кнопку **Сохранить** в окне параметров виджета.

   Виджет отображается на панели мониторинга.
7. Нажмите на кнопку **Сохранить** в окне настройки панели мониторинга.

Редактирование виджета

Чтобы изменить виджет:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. Раскройте список панелей мониторинга в верхнем левом углу окна.
3. Выберите панель мониторинга и нажмите на кнопку **Изменить**.

   Откроется окно изменения параметров панели мониторинга.
4. На виджете, который вы хотите изменить, нажмите на значок меню ⋮.
5. Выберите **Изменить**.

   Откроется окно параметров виджета.
6. Задайте параметры виджета.
7. Нажмите на кнопку **Сохранить** в окне параметров виджета.
8. Нажмите на кнопку **Сохранить** в окне настройки панели мониторинга.

Изменения виджета будут применены.

Удаление виджета

Чтобы удалить виджет:

1. В веб-интерфейсе KUMA выберите раздел **Панели мониторинга**.
2. Раскройте список панелей мониторинга в верхнем левом углу окна.

3. Выберите панель мониторинга и нажмите на кнопку **Изменить**.

   Откроется окно изменения параметров панели мониторинга.

4. На виджете, который вы хотите удалить, нажмите на значок меню ⋮.

5. Выберите **Удалить**.

6. В отобразившемся окне подтверждения нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**.

Виджет будет 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
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**. • **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**.

Параметр	Описание
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 редактировать 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)
	
	Результат:
	
	url count
	
	google.com 3
	
	ya.ru 2
	
	mail.ru 1
	
	yandex.ru 1
	
	В KUMA поддержаны следующие функции, которые позволяют использовать в запросах массивы:
	• `groupArray` — собирает все значения аргумента x в массив и используется в агрегатных функциях при группировке данных.
	• `arrayJoin` — раскрывает массив на отдельные строки в результате выполнения запроса.
	При составлении SQL-запроса вы можете использовать переменные. Переменные можно указывать только при составлении запроса вручную. В конструкторе SQL переменные использовать нельзя.
	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 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)`.
	
	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`.

Параметр	Описание
	• При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать неправильно. Мы рекомендуем 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 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 выберете 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**.

    Период рассчитывается относительно настоящего времени.

  - Если вы хотите указать **пользовательский период**, задайте 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. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. 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 и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также 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 Kaspersky SIEM хранится в UTC, но в веб-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 в UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 в 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 для виджета вы включили параметр **Показывать данные за предыдущий период**, и данные на виджете отображаются за относительный период, во всплывающей подсказке также будет отображаться предыдущий период. Предыдущий период рассчитывается относительно текущего периода как значения начала и конца текущего периода минус длительность 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 вам потребуется ввести значение вручную, выбрать его в раскрывающемся списке или выбрать 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**.

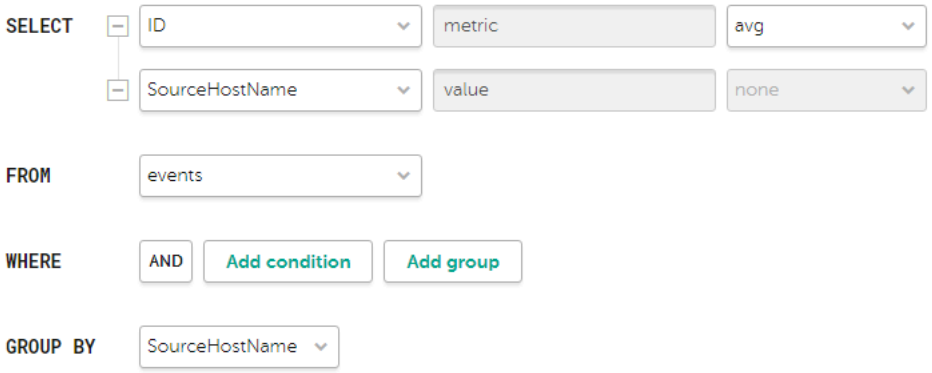
e. **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

- 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 типа **Календарная диаграмма** и **Счетчик**.

2. Нажмите на кнопку **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
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**.
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	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. Параметр доступен для графиков типа **Круговая диаграмма**, **Столбчатая диаграмма** и **Календарная диаграмма**. По умолчанию переключатель выключен.
Длительность отрезков периода	Длительность отрезков, на которые требуется делить период. Доступно для графика типа **Календарная диаграмма**.
Шкала	Шкала для отображения данных. Доступно для графика 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 щелчку 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
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: • **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 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.

Параметр	Описание
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. Пример: 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. Добавление в корреляционное правило действия над активными листами, с помощью которого значение ранее созданной переменной будет с помощью функции **Установить** записываться в активный лист в формате Ключ–Значение. В качестве ключа следует задать поле активного листа (например, `Тенант`), а в поле значения 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

Параметры	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
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 их оптимального отображения.
Итоговые значения	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. Параметр доступен для графиков типа **Круговая диаграмма** и **Столбчатая диаграмма**. По умолчанию переключатель выключен.
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 параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, значение которых требуется указать 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: • **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.

Параметр	Описание
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. Пример: `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 неправильно. 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. Добавление в корреляционное правило действия над активными листами, с помощью которого значение ранее созданной переменной будет с помощью функции **Установить** записываться в активный лист в формате Ключ–Значение. В качестве ключа следует задать поле активного листа (например, `Тенант`), а в поле значения 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

Параметр	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

Параметры	Описание
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	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. Параметр доступен для графиков типа **Круговая диаграмма** и **Столбчатая диаграмма**. По умолчанию переключатель выключен.
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**. • **Сложенная столбчатая диаграмма**. 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 **Сложенная столбчатая диаграмма**. 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 **Сложенная столбчатая диаграмма**. 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**.

Описание параметров

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.

Параметр	Описание
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 **Сложенная столбчатая диаграмма**. 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.

Виджет Изображение

Виджет позволяет разместить изображение на панели мониторинга или в отчете. Например, вы можете использовать виджет **Изображение** для оформления логотипа компании на панели мониторинга или в отчете.

У виджета **Изображение** отсутствует боковая панель с параметрами настройки.

Чтобы добавить файл изображения, наведите курсор на виджет и нажмите **Загрузить изображение**, в появившемся окне файловой системы выберите нужный файл, после добавления файла в виджет нажмите **Сохранить**.

Вы можете добавить несколько виджетов **Изображение** на панель мониторинга. Путем удержания кнопки (⠿) и перетаскивания можно переместить виджеты по панели мониторинга и расположить виджеты в желаемом порядке.

Вы можете создать панель мониторинга с виджетом **Изображение** без добавления файла изображения, например, для разметки. KUMA сохранит панель мониторинга, а затем вы можете редактировать панель мониторинга с помощью кнопки **Изменить** на панели инструментов, и добавить файлы изображения.

Минимальные размеры виджета: 225x161 пикселей. Максимальные размеры: 465x692 пикселей. С помощью кнопки ( ) вы можете изменять размер изображения на виджете. При изменении размеров изображение не обрезается, а масштабируется относительно размеров виджета.

Максимальный размер файла изображения: 3 МБ.

Поддерживаемые форматы файлов изображения: xbm, tif, pjp, apng, svgz, jpg, jpeg, heif, ico, tiff, webp, jfif, heic, gif, svg, png, bmp, pjpeg, avif.

Скачивание данных виджетов в формате CSV не поддерживается.

Вы можете создать, редактировать, дублировать, удалить виджет.

Виджет Текст

Виджет позволяет разместить произвольный текст на панели мониторинга или в отчете. Например, виджет **Текст** можно использовать для отображения названия или краткого описания панели мониторинга или отчета.

Чтобы добавить или изменить текст, нажмите на виджет. При этом активируется поле ввода и появляется панель, позволяющая отформатировать введенный текст. Вы можете ввести до 2000 символов.

У виджета **Текст** отсутствует боковая панель с параметрами настройки. Такой виджет нельзя выгрузить в формат CSV.

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.
- Сложенная столбчатая диаграмма.
- Спидометр.

Параметры для круговых диаграмм

В таблице ниже представлены параметры для графиков типа **Круговая диаграмма**.

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.
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	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. По умолчанию переключатель выключен.
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
Название	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
Название	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, сложенных 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
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**.
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
Название	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.

Параметр	Описание
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 более удобного отображения данных.
Итоговые значения	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. По умолчанию переключатель выключен.
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	Длительность отрезков, на которые требуется делить период. Доступно для графика типа **Календарная диаграмма**.

Параметры для графиков типа Спидометр

В таблице ниже представлены параметры для графиков типа **Спидометр**.

> Значения на графике указываются в процентах.

Описание параметров

Параметр	Описание
Вкладка **Общие**	
Название	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.
Пороговые значения	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 графиков типа **Круговая диаграмма**, **Счетчик**, **Таблица**, **Столбчатая диаграмма**, **Сложенная столбчатая диаграмма**, **Календарная диаграмма** вы можете настроить период отображения данных на виджете с помощью параметра **Период**. По умолчанию период отображения данных в виджете совпадает с периодом отображения данных на 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 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 выберете 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**.

    Период рассчитывается относительно настоящего времени.

- Если вы хотите указать **пользовательский период**, задайте 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. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. 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 и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также 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 Kaspersky SIEM хранится в UTC, но в веб-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 в UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 в 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 для виджета вы включили параметр **Показывать данные за предыдущий период**, и данные на виджете отображаются за относительный период, во всплывающей подсказке также будет отображаться предыдущий период. Предыдущий период рассчитывается относительно текущего периода как значения начала и конца текущего периода минус длительность 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.

  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.

- 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 вы настроите действия по щелчку 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, `Тенант`), а в поле значения 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.

Работа с алертами

Алерты создаются при получении последовательности событий, запускающей правило корреляции. Подробнее об алертах вы можете посмотреть в этом разделе.

В разделе **Алерты** веб-интерфейса KUMA можно просматривать и обрабатывать алерты, зарегистрированные решением. Алерты можно фильтровать. По нажатию на название алерта открывается окно со сведениями о нем.

Формат даты алерта зависит от языка локализации, выбранного в параметрах решения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Жизненный цикл алертов

Ниже представлен жизненный цикл алерта:

1. KUMA создает алерт при срабатывании правила корреляции. Алерт именуется по породившему его правилу корреляции. Алерту присваивается статус **Новый**.

   > Алерты в статусе **Новый** продолжают обновляться данными при срабатывании правил корреляции. Если статус алерта меняется на любой другой, алерт больше не обновляется новыми событиями и, если правило корреляции срабатывает снова, создается новый алерт.

2. Сотрудник службы безопасности назначает оператора для расследования алерта. Статус алерта меняется на **Назначен**.
3. Оператор выполняет одно из следующих действий:
   - Закрывает алерт как ложно положительный (статус алерта меняется на **Закрыт**).
   - Реагирует на угрозу и закрывает алерт (статус алерта меняется на **Закрыт**).
   - Создает на основе алерта инцидент (статус алерта меняется на **В инцидент**).

Наполнение алертов событиями

По умолчанию количество привязанных событий к алерту не может превышать 10 000. Когда количество событий привязанных к алерту достигает 10 000, создается новый алерт с таким же названием, но новым идентификатором. Идентификатор алерта можно просмотреть в деталях алерта. При необходимости вы можете изменить это значение в свойствах правила сегментации в поле **Количество корреляционных событий**. Правило сегментации при этом должно быть включено и привязано к правилам корреляции алертов тенанта.

Разделение алертов

С помощью правил сегментации поток однотипных корреляционных событий можно разделять, создавая более одного алерта.

Настройка таблицы алертов

В основной части раздела **Алерты** отображается таблица с информацией о зарегистрированных алертах.

В таблице алертов отображаются следующие столбцы:

- Уровень важности ( ) – степень значимости потенциальной угрозы безопасности: критическая , высокая , средняя , низкая .
- **Название** – имя алерта.
- **Статус** – текущее состояние алерта:
  - **Новый** – новый, еще не обработанный алерт.
  - **Назначен** – алерт обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – алерт закрыт. Алерт был ложный или угроза безопасности устранена.
  - **Эскалирован** – на основе этого алерта был создан инцидент.
- **Назначен** – имя сотрудника службы безопасности, которому алерт передан для расследования или реагирования.
- **Инцидент** – название инцидента, к которому привязан алерт.
- **Дополнительная информация** – значение поля, выбранного для отображения в разделе **Информация об алерте** при настройке параметров наполнения алерта. При выборе некоторых полей (например, **SourceAddress**, **DestinationAddress**, **SourceUserName**, **DestinationUserName**) дополнительно отображаются связанные с ними поля (**SourceAssetName**, **DestinationAssetName**, **SourceAccountName**, **DestinationAccountName**). Значения этих полей объединяются и отображаются в столбце **Дополнительная информация** через запятую в следующем порядке: сначала выбранное поле, затем дополнительное.

  > Для выбранного поля отображается самое раннее зафиксированное и непустое значение поля события, связанного с алертом.

  По умолчанию столбец не отображается в таблице. Чтобы добавить его, нужно нажать на значок в виде шестеренки ( ) и установить флажок рядом с названием столбца. .
- **Первое появление** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.

- **Категории** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Тенант** – название тенанта, которому принадлежит алерт.
- **КИИ** – указание на то, относятся ли к алерту активы, являющиеся объектами КИИ. Столбец скрыт от пользователей, не имеющих прав доступа к объектам КИИ.

По нажатию на заголовки столбцов вы можете просмотреть инструменты для фильтрации алертов. При фильтрации алертов по какому-либо параметру соответствующий заголовок таблицы алертов подсвечивается желтым цветом.

Нажав на значок в виде шестеренки ( ), вы можете настроить отображаемые столбцы таблицы алертов.

В поле **Поиск** можно вести поиск алертов по связанным с ними активам, пользователям, тенантам или корреляционным правилам. Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.
- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

Фильтрация алертов

В KUMA в разделе **Алерты** можно делать выборки алертов с помощью инструментов фильтрации и сортировки.

Параметры фильтра можно сохранить. Существующие фильтры можно удалить.

Сохранение и выбор фильтра алертов

В KUMA можно сохранять изменения параметров таблицы алертов в виде фильтров. Фильтры сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

Чтобы сохранить текущие параметры фильтра:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите **Сохранить текущий фильтр**.

   Появится поле для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
3. Введите название фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.
4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Фильтр сохранен.

Чтобы выбрать ранее сохраненный фильтр:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите нужный фильтр.

   Чтобы выбрать фильтр, который будет использоваться по умолчанию, поставьте в раскрывающемся списке **Фильтры** звездочку левее названия требуемого фильтра.

Фильтр выбран.

Чтобы сбросить текущие настройки фильтра,

откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтры**.

Удаление фильтра алертов

Чтобы удалить ранее сохраненные фильтры:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Нажмите значок на фильтре, который требуется удалить.
3. Нажмите **OK**.

Фильтр удален для всех пользователей KUMA.

Просмотр подробной информации об алерте

Чтобы просмотреть информацию об алерте:

1. В окне веб-интерфейса решения выберите раздел **Алерты**.

   Отобразится таблица алертов.
2. Нажмите на название алерта, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об алерте.

В верхней части окна с информацией об алерте расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. В этом окне можно обработать алерт: изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент.

Раздел Информация об алерте

Этот раздел позволяет просмотреть основную информацию об алерте. Он содержит следующие данные:

- **Уровень важности правила корреляции** – уровень важности правила корреляции, в результате срабатывания которого создан алерт.
- **Наивысшая важность категории активов** – самый высокий уровень важности категории активов из тех, которые принадлежат связанным с этим алертом активам. Если с алертом связано несколько активов, отображается наибольшее значение.
- **Привязан к инциденту** – если алерт привязан к инциденту, то отображаются название и статус алерта. Если алерт не привязан к инциденту, поле не заполнено.
- **Первое появление** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.
- **Идентификатор алерта** – уникальный идентификатор алерта в KUMA.
- **Тенант** – название тенанта, которому принадлежит алерт.
- **Правило корреляции** – название правила корреляции, в результате срабатывания которого создан алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.

Также в этом разделе может дополнительно отображаться поле корреляционного события и его значение, выбранное при настройке параметров наполнения алерта в раскрывающемся списке **Отображать в Информации об алерте**. При выборе некоторых полей дополнительно отображаются связанные с ними поля. Например, для поля **SourceAddress** дополнительно отображается поле **SourceAssetName**, для **DestinationAddress** – **DestinationAssetName**, для **DeviceAddress** – **DeviceAssetName**, для **SourceHostName** – **SourceAssetName**, для **DestinationHostName** – **DestinationAssetName**, для **DeviceHostName** – **DeviceAssetName**. При выборе поля **SourceUserName** дополнительно отобразится поле **SourceAccountName**, а при выборе **DestinationUserName** – **DestinationAccountName**. Это работает только в одном направлении, то есть, например, при выборе поля **DestinationAccountName**, поле **DestinationUserName** не отобразится.

> Для выбранного поля отображается самое раннее зафиксированное и непустое значение поля события, связанного с алертом.

Раздел Связанные события

Этот раздел содержит таблицу событий, относящихся к алерту. Если нажать на значок стрелки (›) рядом с правилом корреляции, отобразятся базовые события из этого правила корреляции. События можно сортировать по уровню важности и времени.

При выборе события в таблице открывается область деталей, содержащая информацию о выбранном событии. В области деталей также отображает кнопка **Подробные сведения**, при нажатии на которую открывается окно, содержащее информацию о корреляционном событии.

Ссылки **Найти в событиях** под корреляционными событиями и кнопка **Найти в событиях** справа от заголовка раздела используются для перехода к расследованию алерта.

С помощью кнопки **Скачать события** вы можете скачать информацию о связанных событиях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы, заполненные хотя бы в одном связанном событии.

Некоторые редакторы CSV-файлов воспринимают значение разделителя (например, \n) в экспортируемом из KUMA CSV-файла как перенос строки, а не как разделитель. Может быть нарушено разделение файла на строки. Если вы столкнулись с подобным, то может потребоваться дополнительное редактирование CSV-файла, полученного из KUMA.

В таблице событий, в области деталей событий, в окне алертов, а также в виджетах в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Раздел Связанные активы

Этот раздел содержит таблицу активов, относящихся к алерту. Информация об активах поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные активы. Активы можно сортировать по столбцам **Количество** и **Актив**.

В этом разделе также отображаются активы, связанные с алертом. При нажатии на название актива открывается окно **Информация об активе**. В открывшемся окне в разделе **Связанные алерты** с помощью раскрывающегося списка **Найти связанные алерты** вы можете выбрать период, за который вы хотите найти связанные алерты: за последний день, неделю, две недели (значение по умолчанию), месяц или год. После того как вы выберете период, отобразится количество найденных связанных алертов. Для просмотра полного списка нужно нажать на кнопку **Найти в алертах**, после чего откроется страница **Алерты** с отфильтрованным списком найденных связанных алертов.

С помощью кнопки **Скачать активы** вы можете скачать информацию о связанных активах в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Название**, **IP-адрес**, **Полное доменное имя**, **Категории**.

Раздел Связанные пользователи

Этот раздел содержит таблицу пользователей, относящихся к алерту. Информация о пользователях поступает из событий, связанных с алертом. С помощью поля **Поиск пользователей** можно искать нужных пользователей. Пользователей можно сортировать по столбцам **Количество**, **Пользователь**, **User principal name** (Основное имя пользователя) и **Адрес электронной почты**.

С помощью кнопки **Скачать пользователей** вы можете скачать информацию о связанных пользователях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Пользователь**, **Имя участника-пользователя (UPN)**, **Адрес электронной почты**, **Домен**, **Тенант**.

Раздел Журнал изменений

Этот раздел содержит записи об изменениях, которые пользователи внесли в алерт. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии. Комментарии можно сортировать по столбцу **Время**.

При необходимости в поле **Комментарий** вы можете внести комментарий к алерту и нажать **Добавить**, чтобы сохранить его.

Изменение названия алертов

Чтобы изменить название алерта:

1. В окне веб-интерфейса KUMA выберите раздел **Алерты**.

   Отобразится таблица алертов.

2. Нажмите на название алерта, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

3. В верхней части окна нажмите на значок и в открывшемся поле введите новое название алерта. Подтвердите название, нажав **ENTER** или щелкнув вне поля ввода.

Название алерта изменено.

Настройка параметров наполнения алертов

Чтобы настроить параметры наполнения алертов:

1. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Алерты**.

2. В открывшемся окне **Алерты** перейдите на вкладку **Наполнение алертов** и задайте значение следующих параметров:

   a. В раскрывающемся списке **Статус** выберите значение, при котором алерт будет наполняться событиями. Значение по умолчанию: **Новый**. В можете выбрать несколько значений. Значение **Новый** недоступно для удаления из выборки. Доступные значения:

      - **Новый** – создаваемые корреляционные события продолжают привязываться к алерту только в том случае, если статус алерта **Новый**.

      - **В инциденте** – создаваемые корреляционные события продолжают привязываться к алерту только в том случае, если статус алерта **В инциденте**. Если алерт перешел в статус **В инциденте**, он может вернуться в статус **Новый**, если алерт будет отвязан от инцидента. В этом случае алерт больше не будет наполняться событиями.

        Пример: алерт находится в статусе **В инциденте**. За время пребывания алерта в статусе **В инциденте** новых событий не поступало. Если отвязать алерт от инцидента, алерт будет пополняться событиями. Если, пока алерт был привязан к инциденту, поступали еще события и был создан новый алерт, будет наполняться последний созданный алерт.

      - **Назначен** – создаваемые корреляционные события продолжают привязываться к алерту только в том случае, если статус алерта **Назначен**.

   b. В поле **Алерт создан не позднее (часы)** укажите время, в течение которого алерт будет наполняться событиями. Значение параметра должно быть целым числом. Отсчет времени осуществляется от момента создания алерта. Значение по умолчанию: 336 часов (2 недели). Минимальное значение: 1 час.

      Если указаны значения для параметров **Статус**, **Алерт создан не позднее (часы)** и **Максимальное количество событий**, наполнение алерта прекращается при выполнении первого из следующих условий:

      - статус алерта изменился и больше не соответствует выбранным значениям;

      - истекло заданное время наполнения;

      - количество событий в алерте достигло значения, указанного в поле **Максимальное количество событий**.

      Если после прекращения наполнения алерт снова переходит в статус, при котором наполнение разрешено, новые события в него не добавляются. Например, если наполнение настроено только для статуса **Новый**, после перехода алерта в статус **В инциденте** наполнение прекращается. Если затем алерт снова получает статус **Новый**, новые события в него не добавляются.

c. В раскрывающемся списке **Хранилище событий** выберите хранилище, в котором хранятся события алерта. Можно указать только одно хранилище. В списке отображаются ресурсы хранилища, а не запущенные сервисы. Для того чтобы алерты наполнялись событиями, сервис хранилища должен быть запущен.

   Алерты, созданные до указания хранилища в параметрах наполнения, не содержат события. После того, как значение параметра **Хранилище событий** задано или изменено, существующие алерты не наполняются событиями указанного хранилища. В этом случае создаются новые алерты с событиями указанного хранилища. После выбора хранилища событий, этот параметр может применяется к алертам до двух минут. Алерты созданные до применения этого параметра, могут не содержать события указанного хранилища.

d. В раскрывающемся списке **Отображать в Информации об алерте** выберите поле корреляционного события, которое будет отображаться в карточке алерта и в столбце **Дополнительная информация** в разделе **Алерты**. Вы можете выбрать одно из следующих значений:

   - **DestinationAddress** – IPv4 или IPv6-адрес точки назначения (актива), в отношении которой произошло событие.
   - **SourceAddress** – IPv4 или IPv6-адрес устройства-источника события. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
   - **DeviceAddress** – IPv4 или IPv6-адрес устройства, с которого было получено событие.
   - **DestinationAssetName** – название актива в точке назначения.
   - **SourceAssetName** – название актива на источнике события.
   - **DeviceAssetName** – название актива на устройстве, с которого было получено событие.
   - **DestinationHostName** – доменное имя точки назначения.
   - **SourceHostName** – доменное имя источника события.
   - **DeviceHostName** – имя устройства, с которого было получено событие. FQDN устройства, если доступно.
   - **DestinationUserName** – имя пользователя точки назначения.
   - **SourceUserName** –имя пользователя источника.
   - **DestinationAccountName** – название учетной записи в точке назначения.
   - **SourceAccountName** – название учетной записи источника события.
   - **Message** – краткое описание события.
   - **DeviceCustomString1**, **DeviceCustomString2**, **DeviceCustomString3**, **DeviceCustomString4**, **DeviceCustomString5**, **DeviceCustomString6** – поля для маппинга строкового значения.

   Вы можете выбрать только одно поле. Для некоторых полей автоматически отображается дополнительное связанное поле. Если выбрано поле, которое относится к адресу или имени хоста, дополнительно отображается связанное поле **AssetName**. Если выбрано поле, связанное с именем пользователя, дополнительно отображается поле **AccountName**. В этих случаях значения полей объединяются через запятую: сначала выбранное поле, а затем дополнительное.

   Настроенный параметр применяется только к новым алертам.

e. В поле **Максимальное количество событий** укажите максимальное количество событий, которые могут быть добавлены в один алерт. После достижения указанного количества наполнение алерта прекращается.

   Значение параметра должно быть целым числом. Значение по умолчанию: `10000`. Минимальное значение: `1`. Максимальное значение не ограничено.

   При сохранении правил сегментации выполняется проверка значения количества событий. Если в правиле указано количество событий, превышающее значение параметра Максимальное количество событий, сохранение завершается с ошибкой. Для правил сегментации, созданных до уменьшения значения параметра, изменение не применяется. Такие правила продолжают работать, но количество событий, добавляемых в алерт, не превышает значение параметра **Максимальное количество событий**.

Параметры наполнения алертов настроены.

Обработка алертов

Вы можете изменить уровень важности алерта, назначить алерт пользователю, закрыть алерт или создать на основе алерта инцидент.

Чтобы обработать алерт:

1. Выберите необходимые алерты одним из следующих способов:

   - В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть.

     Откроется окно алерта, в верхней его части расположена панель инструментов.

   - В разделе **Алерты** веб-интерфейса KUMA установите флажок рядом с требуемым алертом. Можно выбрать более одного алерта.

     > Алерты со статусом **Закрыт** не могут быть выбраны для обработки.

     В нижней части окна отобразится панель инструментов.

2. Измените уровень важности алерта с помощью раскрывающегося списка **Уровень важности**:

   - **Низкий**.
   - **Средний**.
   - **Высокий**.
   - **Критический**.

   Уровень важности алерта принимает выбранное значение.

3. Назначьте алерт пользователю с помощью раскрывающегося списка **Назначить**.

   Вы можете назначить алерт себе, выбрав **Мне**.

   Статус алерта изменится на **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.

4. В разделе **Связанные пользователи** выберите пользователя и настройте параметры реагирования через Active Directory.

   a. После выбора связанного пользователя в открывшемся окне **Информация об учетной записи** нажмите **Реагирование через Active Directory**.

   b. В раскрывающемся списке **Команда Active Directory** выберите одно из следующих значений:

      - **Добавить учетную запись в группу**

        Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
        В обязательном для заполнения поле **Distinguished name** 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 необходимо переместить учетную запись.
        В обязательном для заполнения поле **Distinguished name** 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

      - Блокировать учетную запись

   c. Нажмите **Применить**.

5. При необходимости создайте на основе алерта инцидент:

   a. Нажмите **Создать инцидент**.

      Откроется окно создания инцидента. В качестве названия инцидента используется название алерта.

   b. Измените нужны параметры инцидента и нажмите **Сохранить**.

   Инцидент создан, статус алерта изменен на **Эскалирован**. Алерт можно отвязать от инцидента, выбрав его и нажав **Отвязать**.

6. Закройте алерт:

   a. Нажмите **Закрыть алерт**.

      Откроется окно подтверждения.

   b. Укажите причину закрытия алерта:

      - **Отработан**. Это означает, что были приняты необходимые меры по устранению угрозы безопасности.

      - **Неверные данные**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности.

      - **Неверное правило корреляции**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции.

   c. Нажмите **OK**.

Статус алерта изменен на **Закрыт**. Алерты с таким статусом не обновляются новыми корреляционными событиями и отображаются в таблице алертов, только если в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого алерта или назначить его другому пользователю невозможно.

Расследование алерта

Расследование алерта используется, когда вам нужно получить дополнительную информацию об угрозе, из-за которой был создан алерт: реальна ли угроза, откуда она исходит, на какие элементы сетевой среды она влияет, как следует бороться с угрозой. Анализ событий, связанных с корреляционными событиями, которые в свою очередь породили алерт, может помочь вам определить курс действий.

Для обеспечения удобства расследования алертов убедитесь, что на всех устройствах, связанных с жизненным циклом обработки событий (источники событий, серверы KUMA, клиентские хосты) время синхронизируется при помощи серверов Network Time Protocol (NTP).

В KUMA режим расследования алерта включается, когда вы нажимаете ссылку **Найти в событиях** в окне алерта или в окне корреляционного события. В режиме расследования алерта отображается таблица событий с фильтрами, автоматически настроенными на поиск событий из алерта или корреляционного события. Фильтры также соответствуют времени продолжительности алерта или времени регистрации корреляционного события. Вы можете изменить эти фильтры, чтобы найти другие события и узнать больше о процессах, связанных с угрозой.

В режиме расследования алерта становится доступным дополнительный раскрывающийся список :

- **Все события** – просмотр всех событий.
- **События алерта** (выбрано по умолчанию) – просмотр только событий, связанных с алертом.

  При фильтрации событий, связанным с алертом, действуют ограничения на сложность поисковых SQL-запросов.

Вы можете вручную привязать к алертам событие любого типа, кроме корреляционного. К алерту можно привязать только не привязанные к нему события.

В режиме расследования алерта можно создавать и сохранять конфигурации фильтров событий. При использовании этого фильтра в обычном режиме просмотра событий будут отображены все события, соответствующие критериям фильтра, независимо от того, привязаны ли они к алерту, выбранному для расследования алерта.

Чтобы привязать событие к алерту:

1. В разделе **Алерты** веб-интерфейса KUMA нажмите алерт, к которому вы хотите привязать событие.

   Откроется окно алерта.

2. В разделе **Связанные события** нажмите на кнопку **Найти в событиях**.

   Откроется таблица событий с включенными фильтрами даты и времени, соответствующим дате и времени регистрации привязанных к алерту событий. В столбцах отображаются параметры, используемые правилом корреляции для создания алерта. В таблице событий также отображается столбец **Привязка к алерту**, в котором отмечаются события, привязанные к алерту.

3. В раскрывающемся списке выберите значение **Все события**.

4. При необходимости измените фильтры, чтобы найти событие, которое требуется привязать к алерту.

5. Выберите нужное событие и нажмите на кнопку **Привязать к алерту** в нижней части области деталей события.

   Событие будет привязано к алерту. Вы можете отвязать это событие от алерта, нажав в области деталей **Отвязать от алерта**.

Когда событие привязывается или отвязывается от алерта, в окне алерта в разделе **Журнал изменений** добавляется запись об этом действии. По ссылке в этой записи вы можете открыть область деталей и отвязать или привязать событие к алерту, нажав на соответствующую кнопку.

Хранение алертов и инцидентов

Условия хранения алертов и инцидентов определяются следующими критериями:

- Сроком хранения. По умолчанию алерты и инциденты хранятся в KUMA в течение 365 дней, но этот срок можно изменить с помощью параметра **Срок хранения алертов, дни**.

- Условиями удаления. По истечении заданного срока хранения при соблюдении ряда условий алерты и инциденты могут продолжать храниться.

Ограничения на размер хранимого алерта отсутствуют.

Изменение срока хранения алертов и инцидентов

Чтобы изменить срок хранения алертов и инцидентов в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие**.

2. В открывшемся окне **Общие** в блоке параметров **Свойства Ядра** задайте значение параметра **Срок хранения алертов, дни**.

   Срок хранения алертов и инцидентов изменен.

Условия удаления алертов и инцидентов

В KUMA приняты следующие условия удаления алертов и инцидентов:

- Если алерт старше срока хранения, вне зависимости от статуса алерта его события удаляются.

- Если алерт старше срока хранения, находится в статусе **Закрыт** и не привязан к инциденту, алерт удаляется.

- Если алерт старше срока хранения (вне зависимости от статуса алерта) и привязан к инциденту, срок хранения которого еще не истек, события алерта удаляются, алерт без событий доступен для отображения и остается привязанным к инциденту без событий.

- Если инцидент старше срока хранения, статус инцидента **Закрыт** и у него нет привязанных алертов, инцидент удаляется.

- Если инцидент старше срока хранения, статус инцидента **Закрыт** и к нему привязаны только алерты старше срока хранения (статус алертов, привязанных к закрытому инциденту всегда **Closed, incident closed**), инцидент вместе со всеми алертами и событиями удаляется.

- Если инцидент старше срока хранения (вне зависимости от статуса инцидента) и к нему привязаны алерты, срок хранения которых еще не истек, не удаляется ничего.

- Если инцидент старше срока хранения, в статусе отличном от **Закрыт** и к нему привязаны алерты с истекшим сроком хранения, инцидент не удаляется, алерты не удаляются, события алертов удаляются.

- Пустые алерты (алерты без событий, срок хранения которых истек) удаляются вместе с инцидентами, когда для инцидента наступят условия удаления по сроку хранения (инцидент в статусе **Закрыт** и его срок хранения истек).

- Если инцидент старше срока хранения, статус инцидента **Закрыт**, к нему привязаны алерты старше срока хранения и алерты, срок хранения которых еще не истек, инцидент не удаляется. Алерты, срок хранения которых еще не истек, не удаляются. События алертов, срок хранения которых подошел к концу, удаляются, а сами алерты остаются пустыми и привязанными к инциденту.

Уведомления об алертах

При создании и назначении алертов по электронной почте рассылаются стандартные уведомления KUMA. Вы можете настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона электронной почты.

Создание правила уведомлений

Чтобы настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона:

1. Откройте раздел **Параметры** → **Другое** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA.

2. Выберите тенант, для которого вы хотите создать правило уведомления:

   - Если у тенанта уже есть правила уведомлений, выберите его в таблице.

   - Если у тенанта нет правил уведомлений, нажмите **Добавить параметры для нового тенанта**.

3. В открывшемся окне **Параметры правил уведомлений** настройте следующие параметры:

   - Если вы хотите, чтобы правило было применено после сохранения параметров, переведите переключатель **Состояние** в активное положение.

   - В раскрывающемся списке **Тенант** выберите нужный тенант.

4. В блоке параметров **Правила уведомлений** нажмите **Добавить** и укажите параметры правила уведомлений:

   - **Название** (обязательно) – в этом поле укажите название правила уведомления.

   - **Адреса получателей** (обязательно) – в этом блоке параметров с помощью кнопки **Адрес электронной почты** можно добавить адреса электронной почты, на которые необходимо отправлять уведомления о создании алертов. Адреса добавляются по одному.

     Адреса электронной почты должны содержать только символы ASCII.

   - **Правила корреляции** (обязательно) – в этом блоке параметров необходимо выбрать одно или несколько правил корреляции, при срабатывании которых будут отправляться уведомления.

     В окне в виде древовидной структуры отображаются правила корреляции из общего и выбранного пользователем тенанта. Для выбора правила необходимо установить флажок рядом с ним. Можно установить флажок рядом с папкой: в таком случае будут выбраны все правила корреляции в этой папке и ее подпапках.

   - **Шаблон** (обязательно) – в этом блоке параметров необходимо выбрать шаблон уведомлений, по которому будут создаваться рассылаемые уведомления. Для выбора шаблона нажмите на значок , в открывшемся окне выберите требуемый шаблон и нажмите **Сохранить**.

     Шаблон можно создать, нажав на значок плюса, или отредактировать выбранный шаблон, нажав на значок карандаша.

   - **Выключено** – установив этот флажок вы можете выключить правило уведомления.

5. Нажмите **Сохранить**.

Правило уведомления создано. Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

Дублирование параметров правила уведомлений

Чтобы дублировать параметры уведомлений о создании алерта:

1. Откройте правила уведомлений:

   a. В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Алерты** → **Правила уведомлений**.

   b. В таблице тенантов выберите тенант, параметры правила уведомлений которого которого вы хотите дублировать. При выборе тенанта откроется окно **Параметры правила уведомлений**.

2. Скопируйте параметры исходного правила:

   a. В открывшемся окне **Параметры правила уведомлений** в блоке **Правила уведомлений** откройте нужное правило.

      Откроется окно **Изменить правило уведомлений**.

b. В окне **Изменить правило уведомлений** нажмите кнопку **Копировать**.

   Кнопка **Вставить** становится доступной только после нажатия на кнопку **Копировать**.

   Копирование возможно в рамках одного тенанта и между разными тенантами.

c. Нажмите на кнопку (×) или нажмите **Отмена**, чтобы закрыть окно **Изменить правило уведомлений**.

3. Подготовка к вставке:

   - Если вы хотите дублировать параметры в рамках того же тенанта, переходите к следующему шагу.
   - Если вы хотите использовать скопированные параметры в другом тенанте:
     1. Закройте окно **Параметры правила уведомлений** текущего тенанта.
     2. Перейдите к нужному тенанту. При выборе тенанта откроется окно **Параметры правила уведомлений**.

4. Вставка параметров:

   a. В окне **Параметры правила уведомлений** нажмите **Добавить**.

   b. В открывшемся окне **Изменить правило уведомлений** нажмите кнопку **Вставить**.

5. Проверка и редактирование полей. После вставки следующие параметры будут продублированы, а соответствующие поля предзаполнены:

   - **Состояние** — переключатель будет установлен в том же положении, что в исходном правиле.
   - **Название** — введите новое имя правила. Сохранение копии с тем же названием, что у исходного правила, невозможно.
   - **Адреса получателей** — список получателей будет продублирован. При необходимости его можно изменить.
   - **Тенанты и правила корреляции**.

     Поведение дерева правил корреляции зависит от принадлежности правила уведомлений к тенанту:

     - Если копирование и вставка параметров выполняется в рамках одного тенанта, после вставки в дереве правил корреляции будут автоматически выбраны правила корреляции из исходного правила уведомлений.
     - Если копирование и вставка выполняется в рамках разных тенантов, но правило корреляции размещено в Shared-тенанте, после вставки в дереве правил корреляции будут автоматически выбраны правила корреляции из исходного правила уведомлений.
     - Если копирование и вставка выполняется в рамках разных тенантов, а правило корреляции размещено не в Shared-тенанте, после вставки вернется ошибка доступа. В этом случае необходимо вручную указать тенант и правила корреляции.
   - **Шаблон** — будет указан тот же шаблон, что и в исходном правиле.

   При необходимости измените вставленные параметры.

6. Нажмите **Сохранить**.

Параметры правила уведомлений продублированы.

Выключение правила уведомлений

Чтобы выключить правила уведомлений для тенанта:

1. Откройте раздел **Параметры** → **Другое** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA и выберите тенант, правила уведомлений которого вы хотите выключить.

2. Установите флажок **Выключено**.

3. Нажмите **Сохранить**.

Правила уведомлений выбранного тенанта выключены.

> Для выключенных правил уведомлений не проверяется корректность указанных параметров, при этом включить уведомления для тенанта при наличии некорректных правил невозможно. Если вы при выключенных правилах уведомлений для тенанта создаете или редактируете отдельные правила уведомлений, перед включением правил уведомлений для тенанта рекомендуется: 1) выключить все отдельные правила уведомлений; 2) включить правила уведомлений для тенанта; 3) включить отдельные правила уведомлений по одному.

Работа с инцидентами

В разделе **Инциденты** веб-интерфейса KUMA можно создавать, просматривать и обрабатывать инциденты. При необходимости вы также можете фильтровать инциденты. При нажатии на название инцидента открывается окно со сведениями о нем.

Инциденты можно экспортировать в НКЦКИ.

Срок хранения инцидентов составляет один год, однако этот параметр можно изменить.

Формат даты инцидента зависит от языка локализации, выбранного в параметрах решения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.

- Русская локализация: ДД.ММ.ГГГГ.

О таблице инцидентов

В основной части раздела **Инциденты** отображается таблица с информацией о зарегистрированных инцидентах. При необходимости вы можете изменить набор столбцов и порядок их отображения в таблице.

Как настроить таблицу инцидентов

1. В правом верхнем углу таблицы инцидентов нажмите на значок шестеренки (⚙).

   Откроется окно настройки таблицы.

2. Установите флажки напротив тех параметров, которые требуется отображать в таблице.

   Когда вы устанавливаете флажок, таблица событий обновляется и добавляется новый столбец. При снятии флажка столбец исчезает.

   С помощью поля **Поиск** можно искать параметры таблицы.

   При нажатии на кнопку **По умолчанию** для отображения выбираются следующие столбцы:

   - **Название**.
   - **Длительность инцидента**.
   - **Назначен**.
   - **Создано**.
   - **Тенант**.
   - **Статус**.
   - **Количество обнаружений**.
   - **Уровень важности**.
   - **Категории затронутых активов**.

3. При необходимости измените порядок отображения столбцов, перетащив заголовки столбцов.

4. Чтобы отсортировать инциденты по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

5. Чтобы отфильтровать инциденты по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите требуемые фильтры. Набор фильтров, доступный в раскрывающемся списке, зависит от выбранного столбца.

6. Чтобы снять фильтры, нажмите на заголовок нужного столбца и выберите **Очистить фильтр**.

Доступные столбцы таблицы инцидентов:

- **Название** – название инцидента. Инциденты, поступившие от НКЦКИ, содержат в названии префикс ALRT*.
- **Длительность инцидента** – время, на протяжении которого происходил инцидент (время между первым и последним событием, относящимся к инциденту).
- **Назначен** – имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.

- **Создан** – дата и время создания инцидента. С помощью этого столбца инциденты можно фильтровать по времени их создания.
  - Доступны преднастроенные периоды: **Сегодня**, **Вчера**, **На этой неделе**, **На прошлой неделе**.
  - При необходимости можно задать произвольный период с помощью календаря, который открывается при выборе пунктов **До даты**, **После даты**, **В течение периода**.
- **Тенант** – название тенанта, которому принадлежит инцидент.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.
- **Количество алертов** – количество алертов, входящих в инцидент. Учитываются только алерты тех тенантов, к которым у вас есть доступ.
- **Уровень важности** – степень значимости потенциальной угрозы безопасности: **Критический** , **Высокий** , **Средний** , **Низкий** .
- **Категории затронутых активов** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Последнее обновление** – дата и время последнего изменения, сделанного в инциденте.
- **Первое событие** и **Последнее событие** – дата и время первого и последнего события в инциденте.
- **Категория инцидента** и **Тип инцидента** – категория и тип угрозы, присвоенные инциденту.
- **Экспорт в НКЦКИ** – статус экспорта данных об инциденте в НКЦКИ:
  - **Не экспортировался** – данные не передавались в НКЦКИ.
  - **Ошибка экспорта** – попытка передать данные в НКЦКИ завершилась ошибкой, данные не переданы.
  - **Экспортирован** – данные об инциденте успешно переданы в НКЦКИ.
- **Ветвь** – данные о том, в каком узле был создан инцидент. По умолчанию отображаются инциденты вашего узла. Этот столбец отображается только при включенном режиме иерархии.
- **КИИ** – указание на то, относятся ли к инциденту активы, являющиеся объектами КИИ. Столбец скрыт от пользователей, не имеющих прав доступа к объектам КИИ.

В поле **Поиск** можно ввести регулярное выражение для поиска инцидентов по связанным с ними активами, пользователям, тенантам, корреляционным правилам или категориям затронутых активов. Параметры, по которым производится поиск:

- Активы: название, идентификатор, FQDN, IP-адрес, MAC-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.

- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название. Вы можете выбрать одно или несколько значений из списка тенантов.
- Категории затронутых активов. Вы можете выбрать одну или несколько категорий с указанием уровня важности.

При фильтрации инцидентов по какому-либо параметру соответствующий столбец в таблице инцидентов подсвечивается желтым цветом.

Сохранение и выбор конфигураций фильтра инцидентов

В KUMA можно сохранять изменения параметров таблицы инцидентов в виде фильтров. Конфигурации фильтров сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

Чтобы сохранить текущие параметры конфигурации фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.
2. Выберите **Сохранить текущий фильтр**.

   Откроется окно для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
3. Введите название конфигурации фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.
4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.
2. Выберите нужную конфигурацию.

Конфигурация фильтра активна.

Вы можете выбрать фильтр, который будет использоваться по умолчанию, поставив в раскрывающемся списке **Фильтры** звездочку левее названия требуемой конфигурации фильтра.

Чтобы сбросить текущие настройки фильтра,

откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтр**.

Удаление конфигураций фильтра инцидентов

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Фильтры**.
2. Нажмите значок рядом с фильтром, который требуется удалить.
3. Нажмите **OK**.

   Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр подробной информации об инциденте

Чтобы просмотреть информацию об инциденте:

1. В окне веб-интерфейса решения выберите раздел **Инциденты**.
2. Выберите инцидент, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об инциденте.

Некоторые параметры инцидентов доступны для редактирования. Инциденты, автоматически созданные в KUMA по результатам уведомления от НКЦКИ, содержат префикс ALRT*.

В верхней части окна информации об инциденте расположена панель инструментов и указано имя пользователя, которому назначен инцидент, а также указаны разделы окна в виде закладок, при нажатии на которые можно перемещаться к нужному разделу. В этом окне вы можете обработать инцидент: назначить его пользователю, объединить его с другим инцидентом или закрыть.

Раздел **Описание** содержит следующие данные:

- **Создан** – дата и время создания инцидента.
- **Название** – название инцидента.

  Название инцидента можно изменить, введя в поле новое название и нажав **Сохранить**. Название должно содержать от 1 до 128 символов в кодировке Unicode.
- **Тенант** – название тенанта, которому принадлежит инцидент.

  Тенанта можно изменить, выбрав необходимый тенант в раскрывающемся списке и нажав **Сохранить**.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.

- **Уровень важности** – значимость угрозы, которую представляет инцидент. Возможные значения:
  - **Критический**.
  - **Высокий**.
  - **Средний**.
  - **Низкий**.

  Уровень важности можно изменить, выбрав нужное значение в раскрывающемся списке и нажав **Сохранить**.

- **Категории затронутых активов** – категории, к которым принадлежат связанные с инцидентом активы.

- **Появление первого события** и **Появление последнего события** – дата и время первого и последнего события в инциденте.

- **Тип инцидента** и **Категория инцидента** – тип и категория угрозы, присвоенная инциденту. Значения можно изменить, выбрав в раскрывающемся списке нужное и нажав **Сохранить**.

- **Экспорт в НКЦКИ** – сведения о том, экспортировался ли этот инцидент в НКЦКИ.

- **Описание** – описание инцидента.

  Описание можно изменить, введя в поле новый текст и нажав **Сохранить**. Описание должно содержать не более 256 символов в кодировке Unicode.

- **Связанные тенанты** – тенанты, относящиеся к связанным с инцидентом алертам, активам и пользователям.

- **Доступные тенанты** – тенанты, алерты которых можно привязывать к инциденту автоматически.

  Список доступных тенантов можно изменить, установив в раскрывающемся списке флажки напротив нужных тенантов и нажав **Сохранить**.

Раздел **Связанные алерты** содержит таблицу алертов, относящихся к инциденту. При нажатии на название алерта открывается окно с подробными данными об этом алерте.

Разделы **Связанные активы** и **Связанные пользователи** содержат таблицы с данными об активах и пользователях, относящихся к инциденту. Эта информация поступает из алертов, связанных с инцидентом.

Таблицы в разделах **Связанные алерты**, **Связанные активы** и **Связанные пользователи** можно дополнить данными, нажав в нужном разделе на кнопку **Привязать** и выбрав в открывшемся окне объект, который следует привязать к инциденту. При необходимости вы можете отвязать объекты от инцидента. Для этого вам требуется выбрать необходимые объекты, нажать **Отвязать** в разделе, к которому они относятся, и сохранить изменения. Если объекты добавлены в инцидент автоматически, их нельзя отвязать, пока не отвязан алерт, в котором они упоминаются. Состав полей в таблицах этих разделов можно изменить, нажав в нужном разделе на кнопку шестеренки (⚙). По данным в таблицах этих разделов можно вести поиск с помощью полей **Поиск**.

Раздел **Журнал изменений** содержит записи об изменениях, которые вы и пользователи вносили в инцидент. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии.

В разделе **Интеграция с НКЦКИ** можно отслеживать статус инцидента в НКЦКИ. Кроме того, в этом разделе можно экспортировать данные об инциденте в НКЦКИ, пересылать в НКЦКИ файлы, а также обмениваться со специалистами НКЦКИ сообщениями.

Если в параметры инцидента на стороне НКЦКИ были внесены изменения, в окне инцидента в KUMA будет отображаться соответствующее уведомление. При этом для параметров, по которым есть расхождения, в окне будут отображаться варианты значений и из KUMA, и из НКЦКИ.

Создание инцидента

Чтобы создать инцидент:

1. Откройте веб-интерфейс KUMA и выберите раздел **Инциденты**.
2. Нажмите **Создать инцидент**.

   Откроется окно создания инцидента.
3. Заполните обязательные параметры инцидента:
   - В поле **Название** введите название инцидента. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит создаваемый инцидент.
4. При необходимости укажите другие параметры инцидента:
   - В раскрывающемся списке **Уровень важности** выберите степень угрозы, которую представляет инцидент. Доступные значения: **Низкий**, **Средний**, **Высокий**, **Критический**.
   - В полях **Появление первого события** и **Появление последнего события** укажите временной диапазон, в котором были получены события, относящиеся к инциденту.
   - В раскрывающихся списках **Категория инцидента** и **Тип инцидента** выберите категорию и тип инцидента. Доступные типы инцидента зависят от выбранной категории.
   - Добавьте **Описание** инцидента. Описание должно содержать не более 256 символов в кодировке Unicode.
   - В раскрывающемся списке **Доступные тенанты** выберите тенанты, алерты которых можно будет привязывать к инциденту автоматически.
   - В разделе **Связанные алерты** добавьте алерты, относящиеся к инциденту.

     Привязка алертов к инцидентам

     Чтобы привязать алерт к инциденту:

     1. В разделе **Связанные алерты** окна инцидента нажмите **Привязать**.

        Откроется окно со списком непривязанных к инцидентам обнаружений.
     2. Выберите требуемые алерты.

        Алерты можно искать по пользователям, активам, тенантам и корреляционным правилам с помощью регулярных выражений PCRE.
     3. Нажмите **Привязать**.

     Алерты связаны с инцидентом и отображаются в разделе **Связанные алерты**.

Чтобы отвязать алерты от инцидента:

1. Выберите нужные алерты в разделе **Связанные алерты** и нажмите на кнопку **Отвязать**.
2. Нажмите **Сохранить**.

   Алерты отвязаны от инцидента. Также алерт можно отвязать от инцидента в окне алерта с помощью кнопки **Отвязать**.

- В разделе **Связанные активы** добавьте активы, относящиеся к инциденту.

  Привязка активов к инцидентам

  Чтобы привязать актив к инциденту:

  1. В разделе **Связанные активы** окна инцидента нажмите **Привязать**.

     Откроется окно со списком активов.
  2. Выберите нужные активы.

     Активы можно искать с помощью поля **Поиск**.
  3. Нажмите **Привязать**.

     Активы связаны с инцидентом и отображаются в разделе **Связанные активы**.

  Чтобы отвязать активы от инцидента:

  1. Выберите нужные активы в разделе **Связанные активы** и нажмите на кнопку **Отвязать**.
  2. Нажмите **Сохранить**.

     Активы отвязаны от инцидента.

- В разделе **Связанные пользователи** добавьте пользователей, относящихся к инциденту.

  Привязка пользователей к инцидентам

  Чтобы привязать пользователя к инциденту:

  1. В разделе **Связанные пользователи** окна инцидента нажмите **Привязать**.

     Откроется окно со списком пользователей.
  2. Выберите нужных пользователей.

     Пользователей можно искать с помощью поля **Поиск**.
  3. Нажмите **Привязать**.

     Пользователи связаны с инцидентом и отображаются в разделе **Связанные пользователи**.

Чтобы отвязать пользователей от инцидента:

1. Выберите нужных пользователей в разделе **Связанные пользователи** и нажмите на кнопку **Отвязать**.

2. Нажмите **Сохранить**.

Пользователи отвязаны от инцидента.

- Добавьте **Комментарий** к инциденту.

5. Нажмите **Сохранить**.

Инцидент создан.

Обработка инцидентов

Для обеспечения удобства обработки инцидентов убедитесь, что на всех устройствах, связанных с жизненным циклом обработки событий (источники событий, серверы KUMA, клиентские хосты) время синхронизируется при помощи серверов Network Time Protocol (NTP).

Вы можете назначить инцидент пользователю, объединить инциденты или закрыть инцидент.

Чтобы обработать инцидент:

1. Выберите необходимые инциденты одним из следующих способов:

   - В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, который нужно обработать.

     Откроется окно инцидента, в его верхней части расположена панель инструментов.

   - В разделе **Инциденты** веб-интерфейса KUMA установите флажок рядом с требуемыми инцидентами.

     В нижней части окна отобразится панель инструментов.

2. В раскрывающемся списке **Назначить** выберите пользователя, которому вы хотите назначить инцидент.

   Вы можете назначить инцидент себе, выбрав **Мне**.

   Инциденту будет присвоен статус **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.

3. В разделе **Связанные пользователи** выберите пользователя и настройте параметры реагирования через Active Directory.

   a. После выбора связанного пользователя в открывшемся окне **Информация об учетной записи** нажмите **Реагирование через Active Directory**.

   b. В раскрывающемся списке **Команда Active Directory** выберите одно из следующих значений:

      - **Добавить учетную запись в группу**

        Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
        В обязательном для заполнения поле **Distinguished name** 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 необходимо переместить учетную запись.
  В обязательном для заполнения поле **Distinguished name** 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

- Блокировать учетную запись

c. Нажмите **Применить**.

4. При необходимости измените параметры инцидента.

5. После расследования закройте инцидент:

   a. Нажмите **Закрыть**.

   Откроется окно подтверждения.

   b. Укажите причину закрытия инцидента:

   - **подтвержден**. Это означает, что инцидент был действительным и были приняты необходимые меры по устранению угрозы безопасности.

   - **не подтвержден**. Это означает, что инцидент был ложным, а полученные события не указывают на угрозу безопасности.

   c. Нажмите **Закрыть**.

   Инциденту будет присвоен статус **Закрыт**. Инциденты с таким статусом невозможно редактировать, и они отображаются в таблице инцидентов, только если при фильтрации таблицы в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого инцидента или назначить его другому пользователю невозможно, однако его можно объединить с другим инцидентом.

6. При необходимости объедините выбранные инциденты с другим инцидентом:

   a. Нажмите **Объединить** и в открывшемся окне выберите инцидент, в который следует поместить все данные из выбранных инцидентов.

   b. Подтвердите выбор, нажав **Объединить**.

   Инциденты будут объединены.

Инцидент обработан.

Изменение инцидентов

Чтобы изменить параметры инцидента:

1. В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, параметры которого нужно изменить.

   Откроется окно инцидента.

2. Измените нужные параметры. Для редактирования доступны все параметры инцидента, которые можно задать при его создании.

3. Нажмите **Сохранить**.

Инцидент будет изменен.

Автоматическая привязка алертов к инцидентам

В KUMA можно настроить автоматическую привязку создаваемых алертов к уже существующим инцидентам, если у алертов и инцидентов есть пересечения по относящимся к ним активам или пользователям. Если настройка включена, то при создании алерта решение выполняет поиск инцидентов за указанный период, к которым относятся активы или пользователи из алерта. Кроме того, решение проверяет, чтобы созданный алерт относился к тенантам, указанным в инцидентах в качестве параметра **Доступные тенанты**. Если удовлетворяющий условиям инцидент найден, решение связывает созданный алерт и найденный инцидент.

Чтобы настроить автоматическую привязку алертов к инцидентам:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам**.

2. Установите флажок **Включить** в блоках параметров **Привязка при пересечении по активам** и/или **Привязка при пересечении по пользователям**, в зависимости от того, какие связи необходимо искать между инцидентами и алертами.

3. Задайте **Срок давности создания инцидента** для параметров, по которым необходимо искать связи. Создаваемые алерты будут сравниваться с инцидентами не старше указанного срока.

Автоматическая привязка алертов к инцидентам настроена.

Чтобы выключить автоматическую привязку алертов к инцидентам,

в разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам** установите флажок **Выключено**.

Категории и типы инцидентов

Для удобства работы вы можете присваивать категории и типы. Если инциденту присвоена категория НКЦКИ, его можно экспортировать в НКЦКИ.

Категории и типы инцидентов, которые можно экспортировать в НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ:

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки
	Заражение ВПО
	Захват сетевого трафика
	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
	Использование контролируемого ресурса для проведения атак
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия
Уведомление о наличии уязвимости	Уязвимый ресурс

Категории инцидентов можно просмотреть или изменить в разделе **Параметры** → **Инциденты** → **Типы инцидентов**, где они отображаются в виде таблицы. При нажатии на заголовки столбцов можно менять параметры сортировки таблицы. Таблица содержит следующие столбцы:

- **Категория инцидента** – общий признак инцидента или компьютерной атаки. Таблицу можно фильтровать по значениям этого столбца.
- **Тип инцидента** – класс инцидента или компьютерной атаки.
- **Категория для НКЦКИ** – соответствие типа инцидента номенклатуре НКЦКИ. Невозможно экспортировать в НКЦКИ инциденты, которым присвоены пользовательские типы и категории. Таблицу можно фильтровать по значениям этого столбца.
- **Уязвимость** – указывает ли тип инцидента на уязвимость.
- **Создан** – дата создания типа инцидента.
- **Изменен** – дата изменения типа инцидента.

Чтобы добавить тип инцидента:

1. В разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Типы инцидентов** нажмите **Добавить**.

   Откроется окно создания типа инцидента.

2. Заполните поля **Тип** и **Категория**.
3. Если создаваемый тип инцидента соответствует номенклатуре НКЦКИ, установите флажок **Категория для НКЦКИ**.

4. Если тип инцидента указывает на уязвимость, установите флажок **Уязвимость**.

5. Нажмите **Сохранить**.

Тип инцидента создан.

Взаимодействие с НКЦКИ

В KUMA в рамках взаимодействия с Национальным координационным центром по компьютерным инцидентам (далее "НКЦКИ") можно выполнять следующие действия:

- экспортировать в НКЦКИ инциденты;
- при запросе НКЦКИ дополнять экспортированный инцидент данными;
- отправлять в НКЦКИ файлы;
- обмениваться сообщениями со специалистами НКЦКИ;
- просматривать изменения в параметрах экспортированных инцидентов, сделанных в НКЦКИ;
- обрабатывать инциденты, автоматически созданные KUMA по результатам уведомления от НКЦКИ, с префиксом ALRT*.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Условия взаимодействия с НКЦКИ

Для взаимодействия с НКЦКИ должны выполняться следующие условия:

- лицензия решения включает модуль GosSOPKA;
- настроена интеграция с НКЦКИ;
- в параметрах пользователей, в обязанности которых входит взаимодействие с НКЦКИ, установлен флажок **Может взаимодействовать с НКЦКИ**.

Этапы взаимодействия с НКЦКИ

В KUMA экспорт и обработка инцидентов, экспортированных в НКЦКИ, проходит через следующие этапы:

1. **Создание инцидента и проверка его на соответствие требованиям НКЦКИ**

   Вы можете создать инцидент или получить его из дочернего узла KUMA. Перед отправкой данных в НКЦКИ необходимо убедиться, что категория инцидента соответствует требованиям НКЦКИ

2. **Экспорт инцидента в НКЦКИ**

При успешном экспорте инцидента в НКЦКИ его параметр **Экспорт в НКЦКИ** принимает значение **Экспортирован**. В нижней части окна инцидента становится доступен раздел с чатом с сотрудниками НКЦКИ.

В НКЦКИ полученному от вас инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ** и в автоматических сообщениях чата.

Если в НКЦКИ предоставлены все необходимые данные, инциденту присваивается статус **Проверка НКЦКИ**. Параметры инцидента в таком статусе доступны для изменения, однако обновленные сведения невозможно передать из KUMA в НКЦКИ. Вы можете просмотреть разницу между данными об инциденте в KUMA и в НКЦКИ.

3. **Дополнение данных об инциденте**

   Если сотрудникам НКЦКИ не хватает сведений для обработки инцидента, они могут присвоить ему статус **Требуется дополнение**. В KUMA этот статус отображается в окне инцидента в разделе **Интеграция с НКЦКИ**. Пользователи уведомляются об изменении статуса.

   Если требуется, вы можете прикрепить к инциденту файл.

   Дополнение данных завершается повторным экспортом инцидента в НКЦКИ, при котором необходимо дополнить или изменить ранее отправленные сведения. Из родительского узла KUMA невозможно вносить изменения в инциденты дочерних узлов – это необходимо сделать сотрудникам дочернего узла KUMA.

   При успешном дополнении инцидента данными ему присваивается статус **Проверка НКЦКИ**.

4. **Завершение обработки инцидента**

   Когда сотрудники НКЦКИ обработают инцидент, в НКЦКИ ему будет присвоен статус **Принято решение**. В KUMA этот статус отображается в окне инцидента в разделе **Интеграция с НКЦКИ**.

   При получении этого статуса инцидент в KUMA автоматически закрывается. Взаимодействие с НКЦКИ по данному инциденту через KUMA становится невозможным.

Экспорт данных в НКЦКИ

Чтобы экспортировать инцидент в НКЦКИ:

1. В разделе **Инциденты** веб-интерфейса KUMA откройте инцидент, который вы хотите экспортировать.

2. Нажмите в нижней части окна на кнопку **Экспорт в НКЦКИ**.

3. Если вы не указали категорию и тип инцидента, укажите эти сведения в открывшемся окне и нажмите на кнопку **Экспорт в НКЦКИ**.

   Откроется окно с параметрами экспорта.
   Если вы указали категорию и тип инцидента в карточке инцидента, следует сохранить инцидент перед экспортом в НКЦКИ.

4. Укажите параметры на вкладке **Основные** окна **Экспорт в НКЦКИ**:

5. На вкладке **Основные параметры**, заполните обязательные поля:

   Название компании, **Владелец актива**, Категория инцидента, Тип инцидента, **Описание**, **значение протокола TLP**, **Дата создания инцидента**, **Статус**, **Название информационной системы**, Категория КИИ системы, **Сфера деятельности компании**, **Местоположение**.

   - 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
- WHITE – раскрытие не ограничено;
- GREEN – раскрытие только для сообщества;
- AMBER – раскрытие только для организаций;
- RED – раскрытие только для круга лиц.
- Если вы хотите предоставить информацию об утечке персональных данных, установите флажок **Утечка ПД** - вкладка **Сведения об утечке ПД** станет доступна для заполнения. По умолчанию флажок снят.

  Поля **Наименование оператора**, **ИНН** и **Адрес оператора** заполняются автоматически значениями, указанными при настройке интеграции с НКЦКИ. При этом значения полей доступны для редактирования при подготовке экспорта данных в НКЦКИ.

  Поля об утечке персональных данных доступны для категории **Уведомление о компьютерном инциденте** для следующих типов уведомлений:

  - **Заражение ВПО**
  - **Компрометация учетной записи**
  - **Несанкционированное разглашение информации**
  - **Успешная эксплуатация уязвимости**
  - **Событие не связано с компьютерной атакой**

- **Сведения о продукте** (обязательно) – эта таблица становится доступна, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

  С помощью кнопки **Добавить элемент** можно добавить в таблицу строку. В столбце **Название** требуется указать название программы (например, `MS Office`), а в столбце **Версия** – версию программы (например, `2.4`).

- **Идентификатор уязвимости** – при необходимости укажите идентификатор обнаруженной уязвимости. Например, `CVE-2020-1231`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

- **Наименование и версия уязвимого продукта** – при необходимости укажите наименование и версию уязвимого продукта. Например, `Операционные системы Microsoft и их компоненты`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

6. При необходимости укажите параметры на вкладке **Дополнительно** окна **Экспорт в НКЦКИ**.

   Набор параметров на вкладке зависит от выбранных категории и типа инцидента:

   - **Средство обнаружения инцидента** – укажите название продукта, с помощью которого был зарегистрирован инцидент. Например, `KUMA 1.5`.

   - **Требуется привлечение сил ГосСОПКА** – установите этот флажок, если вам требуется помощь сотрудников ГосСОПКА.

   - **Время завершения инцидента** – укажите дату и время восстановления штатного режима работы контролируемого информационного ресурса (объекта КИИ) после компьютерного инцидента, окончания компьютерной атаки или устранения уязвимости.

   - **Влияние на доступность** – оцените степень последствий инцидента для доступности системы:

     - **Высокое**

     - **Низкое**

     - **Отсутствует**

   - **Влияние на целостность** – оцените степень последствий инцидента для целостности системы:

     - **Высокое**

     - **Низкое**

     - **Отсутствует**

   - **Влияние на конфиденциальность** – оцените степень последствий инцидента для конфиденциальности информации:

     - **Высокое**

     - **Низкое**

     - **Отсутствует**

- **Иные последствия** – укажите иные значимые последствия инцидента.
- **Город** – укажите город, в котором находится ваша организация.

7. Если к инциденту прикреплены активы, можно указать их параметры на вкладке **Технические данные**.

   Эта вкладка становится активной, только если вы установили флажок **Затронутая система имеет подключение к интернету**.

   При необходимости изменить или дополнить сведения, ранее указанные на вкладке **Технические данные**, это следует делать в вашем личном кабинете ГосСОПКА, даже если сотрудники НКЦКИ запросили у вас дополнительные сведения и у вас есть возможность изменить экспортированный инцидент.

   Категории указываемых активов должны соответствовать категории затронутой КИИ системы.

8. Нажмите **Экспорт**.
9. Подтвердите экспорт.

   Сведения об инциденте переданы в НКЦКИ, параметр инцидента **Экспорт в НКЦКИ** меняется на **Экспортирован**. В НКЦКИ полученному от вас инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**.

Изменить данные в экспортированном инциденте возможно, только если сотрудники НКЦКИ запросили у вас дополнительные сведения. Если дополнительные сведения запрошены не были, но вам требуется внести изменения в экспортированный инцидент, это следует делать в вашем личном кабинете ГосСОПКА.

После успешного экспорта инцидента в нижней части экрана отображается кнопка **Сравнение инцидента KUMA с данными в НКЦКИ**, при нажатии на которую открывается окно, где подсвечиваются различия в данных в инциденте между KUMA и НКЦКИ.

Получение инцидентов от НКЦКИ

После обновления до версии 3.4.1 Ядро KUMA при каждом запуске отправляет запрос о наличии новых карточек инцидентов по адресу, указанному в поле URL в настройках интеграции KUMA с НКЦКИ, и затем продолжает отправлять запросы каждые 10 минут. Если в личном кабинете пользователя НКЦКИ появился новый инцидент, KUMA регистрирует инцидент с префиксом ALRT* и дальнейшее взаимодействие с НКЦКИ ведется уже в рамках созданного инцидента.

Взаимодействие с НКЦКИ доступно, даже если в KUMA инцидент переведен в статус **Закрыт**: вы можете менять значения в поле **Статус НКЦКИ** и вести чат с НКЦКИ.

Уведомления о сообщениях от НКЦКИ отправляются на электронную почту пользователей с ролью Главный администратор.

В новом инциденте поля будут заполнены таким же образом, как указано в следующей таблице.

Значения полей в инциденте, полученном от НКЦКИ.

Название поля	Значение
Создан	При создании инцидента в KUMA автоматически указывается дата и время создания. Пример: 2024-10-08 05:32:39
Имя	Идентификатор или регистрационный номер инцидента (сообщения) в ГосСОПКА. Пример: ALRT-xx-xx-xxx

Название поля	Значение
Тенант	Тенант, в котором будут созданы инциденты, полученные от НКЦКИ. По умолчанию, все инциденты создаются в тенанте Main. Можно изменить тенант создания инцидентов в параметрах интеграции с НКЦКИ. Пример: Main.
Статус	Начальный статус инцидента KUMA. Пример: **Открыт**.
Уровень важности	Степень значимости потенциальной угрозы безопасности. Значение по умолчанию: **Критический**. Доступные значения: **Критический**, **Высокий**, **Средний**, **Низкий**.
Категории затронутых активов	Пусто. Значение можно заполнить вручную.
Появление первого события	Пусто. Значение можно заполнить вручную.
Появление последнего события	Пусто. Значение можно заполнить вручную.
Описание	Значение из поля event_description сообщения, которое присылает НКЦКИ. Доступно для редактирования. Пример: сообщение от НКЦКИ.
Связанные тенанты	То же, что и в поле Тенант. Пример: Main.
Доступные тенанты	То же, что и в поле Тенант. Пример: Main.
Связанные алерты	Пусто. Значение можно заполнить вручную.
Связанные активы	Пусто. Значение можно заполнить вручную.
Связанные пользователи	Пусто. Значение можно заполнить вручную.
Журнал изменений	Пусто. Значение можно заполнить вручную.
Раздел Интеграция с НКЦКИ	
Категория	Категория карточки сообщения. Значение из справочника. Возможные значения: Сообщение от НКЦКИ. Поле недоступно для редактирования.
Тип	Тип события ИБ. Значение из справочника. Возможные значения: **Зараженный ресурс**, **Источник email-рассылки модулей ВПО**, **Источник распространения модулей ВПО**, **Центр управления ВПО**, **Элемент инфраструктуры ВПО**, **Замедление работы ресурса**, **Источник эксплуатации уязвимости**, **Источник компрометации учетной записи**, **Участник захвата сетевого трафика**, **Источник несанкционированного доступа**, **Источник несанкционированного изменения информации**, **Источник рассылки спам-сообщений**, **Публикация запрещенной законодательством РФ информации**, **Размещение фишингового ресурса**, **Наличие несанкционированного контента**, **Участник DDoS-атаки**, **Скомпрометированная учетная запись**, **Источник сетевого сканирования**, **Участник мошеннической деятельности**, **Источник угрозы социальной инженерии**, **Уязвимый ресурс**, **Подозрение на фишинговый ресурс**, **Угроза компрометации ПДн**, **Угроза компьютерной атаки**. Поле недоступно для редактирования.
Статус экспорта в НКЦКИ	**Импортирован из НКЦКИ**. Поле недоступно для редактирования.
Раздел Ход обработки сообщения от НКЦКИ	
Статус НКЦКИ	Статус обработки сообщения от НКЦКИ. Значение из справочника. Поле доступно для редактирования. Возможные значения: **Новое**, **В работе**, **Принято решение**, **Взаимодействие завершено**, **Отправлено в архив**.
Результат	Результат принятого решения. Значение из справочника. Поле доступно для редактирования. Возможные значения: **Меры приняты**, **Информация учтена**, **Сведения не подтверждены**.
Раздел Чат с НКЦКИ	
UUID	Уникальный идентификатор сообщения от НКЦКИ.
Компания	Краткое наименование организации субъекта ГосСОПКА.
Категория	Категория карточки сообщения. Значение из справочника. Пример: сообщение от НКЦКИ.
Тип	Тип события ИБ. Значение из справочника. Пример: зараженный ресурс.
Время создания	Дата и время регистрации сообщения от НКЦКИ. Заполняется по правилам стандарта ISO 8601. Используется время UTC.

Название поля	Значение
Время выявления	Дата и время выявления инцидента. Заполняется по правилам стандарта ISO 8601. Используется время UTC.
Время завершения	Дата и время завершения инцидента. Заполняется по правилам стандарта ISO 8601. Используется время UTC.
Последнее обновление	Дата и время последнего обновления карточки сообщения. Заполняется по правилам стандарта ISO 8601. Используется время UTC.
Описание события	Краткое описание события ИБ. Максимум 5000 символов в кодировке Unicode.
Имя владельца	Владелец информационного ресурса. Максимум 5000 символов в кодировке Unicode.
Регистрационный номер	Регистрационный номер сообщения. Пример: ALRT-20-12-2914.
TLP	Ограничительный маркер TLP. Значение из справочника. Возможные значения: **TLP:WHITE**, **TLP:GREEN**, **TLP:AMBER**, **TLP:RED**.
Раздел Технические сведения	
Блок полей **Технические сведения** отображается со значениями полей, полученными из сообщения. Состав полей **Сообщения от НКЦКИ** в блоке **Технические сведения** зависит от Типа события ИБ и для разных инцидентов набор этих полей может отличаться. Обращайте внимание на значения полей в личном кабинете НКЦКИ. Значения не подлежат редактированию.	

Дополнение данных об инциденте по запросу

Если сотрудникам НКЦКИ потребуются дополнительные сведения об инциденте, они могут их у вас запросить. В этом случае в окне инцидента в разделе **Интеграция с НКЦКИ** статус инцидента меняется на **Требуется дополнение**. При этом следующие пользователи KUMA получают по электронной почте уведомления об изменении статуса: пользователь, которому назначен инцидент, и пользователь, экспортировавший инцидент в НКЦКИ.

Если инциденту в НКЦКИ присвоен статус *Требуется дополнение*, в KUMA для этого инцидента вам также доступны следующие действия:

- Загрузка в НКЦКИ файлов.
- Повторный экспорт данных об инциденте в НКЦКИ с изменением или дополнением ранее указанных сведений. Выполнение этого действия завершает дополнение инцидента данными.

Отправка файлов в НКЦКИ

Вы можете приложить файл к инциденту, если инцидент имеет один из следующих статусов НКЦКИ: *Новое*, *В работе*, *Требуется дополнение*, *Принято решение*. Файл будет доступен как в НКЦКИ, так и в веб-интерфейсе KUMA.

При иерархическом развертывании KUMA загружать файлы в НКЦКИ можно только из родительского узла KUMA. При этом в дочерних узлах KUMA видны журнальные записи о загрузке файла.

В журнале изменений инцидента добавляются сообщения о загрузке в НКЦКИ файлов пользователями KUMA. Сообщения о добавлении файлов со стороны НКЦКИ в журнал не заносятся.

Чтобы приложить файл к инциденту:

1. В разделе **Инциденты** веб-интерфейса KUMA откройте инцидент, к которому вы хотите приложить файл.
2. В разделе окна инцидента **Интеграция с НКЦКИ** выберите вкладку **Файл** и нажмите на кнопку **Отправить файл в НКЦКИ**.

   Откроется окно выбора файла.
3. Выберите нужный файл размером не более 50 МБ и подтвердите выбор.

Файл приложен к инциденту. Файл доступен и для сотрудников НКЦКИ, и для пользователей KUMA.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Обмен сообщениями с сотрудниками НКЦКИ

После успешного экспорта инцидента в НКЦКИ в нижней части окна инцидента становится доступен чат с сотрудниками НКЦКИ. Обмениваться сообщениями можно с момента успешного экспорта инцидента до его закрытия в НКЦКИ.

Окно чата с историей сообщений и полем для ввода новых сообщений доступно в разделе окна инцидента **Интеграция с НКЦКИ** на вкладке **Чат**.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Допустимые категории и типы инцидентов НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ:

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки
	Заражение ВПО
	Захват сетевого трафика
	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
	Использование контролируемого ресурса для проведения атак

Категория инцидента	Тип инцидента
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия
Уведомление о наличии уязвимости	Уязвимый ресурс

Уведомления об изменении статуса инцидента в НКЦКИ

При некоторых изменениях статуса или данных инцидента в НКЦКИ пользователи KUMA получают следующие уведомления по электронной почте:

- Уведомление о получении сообщения от НКЦКИ.
- Уведомление о запросе дополнительных данных.
- Уведомление об изменении данных инцидента в НКЦКИ.
- Уведомление об автоматическом закрытии инцидента.

Уведомления получают следующие пользователи:

- Пользователь, которому был назначен инцидент.
- Пользователь, который экспортировал инцидент в НКЦКИ.

Ретроспективная проверка

В обычном режиме коррелятор работает только с событиями, поступающими от коллекторов в реальном времени. **Ретроспективная проверка** 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 **Ретроспективная проверка** для существующих событий, среди которых есть нужный инцидент.

С помощью поискового запроса вы можете определить список событий, для которых будет выполнена ретроспективная проверка, задать период поиска и указать хранилище, в котором нужно искать события. Можно настроить задачу таким образом, чтобы во время ретроспективной проверки событий создавались алерты и применялись правила реагирования.

Чтобы включить ретроспективную проверку:

1. В разделе **События** веб-интерфейса KUMA получите необходимую выборку событий:

   - Выберите хранилище.

     Перед запуском ретроспективной проверки убедитесь, что выбраны нужные кластеры и пространства.

   - Настройте поисковое выражение с помощью конструктора или поискового запроса.

     Перед запуском ретроспективной проверки убедитесь, что в поле SQL-запроса указано нужное выражение.

   - Задайте необходимый период.

     Перед запуском ретроспективной проверки убедитесь, что в поле периода выбран нужный период.

2. В раскрывающемся списке ··· выберите **Ретроспективная проверка**.

   Откроется окно ретроспективной проверки.

3. В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.

   Перед запуском ретроспективной проверки 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 ретроспективной проверки могут появится новые события, которые также будут отправлены в коррелятор. Если коррелятор установлен не в тенанте Main, 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, проверка будет выполнена с применением всех правил корреляции.

5. Если вы хотите, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.

6. Если вы хотите, чтобы в процессе обработки событий создавались алерты, включите переключатель **Создать алерты**.

7. Нажмите на кнопку **Создать задачу**.

Задача ретроспективной проверки создана и отображается в разделе **Диспетчер задач**.

Чтобы просмотреть результаты проверки, в разделе **Диспетчер задач** веб-интерфейса KUMA нажмите на созданную вами задачу и в раскрывающемся списке выберите **Перейти к событиям**.

> Результаты ретроспективной проверки отображают только сформированные корреляционные события. Начало периода в результатах ретроспективной проверки 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 ретроспективной проверки 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 ретроспективной проверки, а также агрегированными и корреляционными событиями, созданными во время обработки. Корреляционные события, созданные ретроспективной проверкой, имеют дополнительное поле ReplayID, в котором хранится уникальный идентификатор выполнения ретроспективной проверки. 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 ретроспективной проверки. Подробнее см. в документации вашего браузера.

При ретроспективной проверке события не обогащаются данными из CyberTrace и Kaspersky Threat Intelligence Portal.

Активные листы обновляются при ретроспективной проверке.

> Ретроспективную проверку невозможно проводить по SQL-запросам, содержащим арифметические выражения или только поля агрегации. Вы можете выполнить ретроспективную проверку 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 ретроспективную проверку по одной из групп.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о KUMA, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании KUMA.

> Kaspersky предоставляет поддержку KUMA в течение жизненного цикла (см. страницу жизненного цикла решения). 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.

При обработке вашего запроса Службе технической поддержки "Лабораторию Касперского" может понадобиться отчет, созданный с помощью утилиты collect.sh. Подробную информацию о работе с утилитой см. в Базе знаний.

REST API

В KUMA можно обращаться из сторонних решений с помощью API. KUMA REST API работает через HTTP и представляет набор методов запрос/ответ. Поддерживается версия REST API v3.

Запросы REST API необходимо отправлять по следующему адресу:

https://<FQDN Ядра KUMA>:<Порт REST API>/api/<Версия API>/<запрос>

Пример:
https://kuma.example.com:7223/api/v3

По умолчанию для запросов используется порт 7223. При необходимости порт можно изменить.

Чтобы изменить порт, используемый для запросов REST API:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-core.service измените следующую строку, подставив нужный порт:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --external :7220 --internal :7210 --rest
   <требуемый номер порта для запросов REST API>
   ```

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-core`

   Для запросов REST API используется новый порт.

Убедитесь, что порт доступен и не закрыт межсетевым экраном.

Заголовок для аутентификации: Authorization: Bearer <токен>

Формат данных по умолчанию: JSON

Формат даты и времени: RFC 3339

Интенсивность запросов: не ограничена

Создание токена

Чтобы сгенерировать токен для пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Сгенерировать токен**.

   Откроется окно **Новый токен**.

3. Если требуется, установите срок действия токена:

   - Установите флажок **Без окончания срока действия**.
   - В поле **Срок действия** с помощью календаря укажите дату и время истечения срока действия создаваемого токена.

4. Нажмите на кнопку **Сгенерировать токен**.

   При нажатии на эту кнопку в области деталей пользователя отображается поле с автоматически созданным токеном. При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

5. Нажмите **Сохранить**.

Токен сгенерирован и может быть использован для API-запросов. Таким же образом можно сгенерировать токен в профиле своей учетной записи.

Настройка прав доступа к API

В KUMA для каждого пользователя можно настроить операции, которые можно выполнять от лица этого пользователя. Права можно настроить только для пользователей, созданных в KUMA.

Чтобы настроить доступные операции для пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Права доступа через API**.

   Откроется окно со списком доступных операций. По умолчанию пользователю доступны все API-запросы.

3. Установите или снимите флажок напротив требуемой операции.

4. Нажмите **Сохранить**.

Доступные операции для пользователя настроены.

Доступные операции можно аналогичным образом настроить в профиле своей учетной записи.

Авторизация API-запросов

Каждый запрос REST API должен включать авторизацию с помощью токена. Пользователь, с помощью чьего токена выполняется API-запрос, должен иметь права на выполнение такого типа запросов.

К каждому запросу должен прилагаться следующий заголовок:

```
Authorization: Bearer <token>
```

Возможные ошибки:

HTTP-код	Описание	Значение поля message	Значение поля details
400	Некорректный заголовок	invalid authorization header	Example: <пример>
403	Токен не существует или пользователь-владелец выключен	access denied	

Стандартная ошибка

Возвращаемые KUMA ошибки имеют следующий формат:

```
type Error struct {
    Message    string      `json:"message"`
    Details    interface{} `json:"details"`
}
```

Операции REST API v3

Открыть справку по REST API

Приложения

В этом разделе представлены приложения к основному тексту документа.

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла KUMA /opt/kaspersky/kuma/kuma, с помощью которого можно вручную запустить или установить компоненты KUMA. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Параметры команд

Команды	Описание
`tools`	Запуск инструментов управления KUMA.
`collector`	Установка, запуск или удаление сервиса коллектора.
`core`	Установка, запуск или удаление сервиса Ядра.
`correlator`	Установка, запуск или удаление сервиса коррелятора.
`agent`	Установка, запуск или удаление сервиса агента.
`help`	Получение информации о доступных командах и параметрах.
`license`	Получение информации о лицензии.
`storage`	Запуск или установка Хранилища.
`version`	Получение информации о версии решения.

Флаги:

`-h`, `--h` используются для получения справочной информации о командах файла kuma. Например: `kuma <компонент> --help`.

Примеры:

- `kuma version` – получение информации о версии установщика KUMA.
- `kuma core -h` – получение справки по команде `core` установщика KUMA.
- `kuma collector --core <адрес сервера, где должен получить свои параметры коллектор> --id <идентификатор устанавливаемого сервиса> --api.port <порт>` используется для запуска установки сервиса коллектора.

Проверка целостности файлов KUMA

Проверить целостность компонентов KUMA вы можете вручную, запустив скрипт, приведенный ниже.

Целостность компонентов KUMA проверяется с помощью набора скриптов, основанных на инструменте integrity_checker, расположенных в директории /opt/kaspersky/kuma/integrity/bin. При проверке целостности используются xml-файлы манифестов из директории /opt/kaspersky/kuma/ntegrity/manifest/*, защищенные криптографической подписью "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами не ниже прав учетной записи kuma.

Проверка целостности выполняется раздельно для компонентов KUMA и должна выполняться раздельно на серверах с соответствующими компонентами. При проверке целостности также проверяется целостность используемого xml-файла.

Чтобы проверить целостность файлов компонентов:

1. Перейдите в директорию, содержащую набор скриптов с помощью команды:

   ```
   cd /opt/kaspersky/kuma/integrity/bin
   ```

2. Выполните одну из команд, в зависимости от того, целостность какого компонента KUMA вы хотите проверить:

   - `./check_all.sh` – компоненты Ядра KUMA и хранилища;
   - `./check_core.sh` – компонент Ядра KUMA;
   - `./check_collector.sh` – компонент коллектора KUMA;
   - `./check_storage.sh` – компонент хранилища;
   - `./check_event_router.sh` – компонент маршрутизатора событий;
   - `./check_kuma_exe.sh <полный путь к файлу kuma.exe без указания имени файла>` – агент KUMA для Windows. Стандартное расположение исполняемого файла агента на устройстве Windows: C:\Program Files\Kaspersky Lab\KUMA\;
   - `./check_linux_agent.sh <полный путь к исполняемому файлу агента KUMA без указания имени файла>` – агент KUMA для Linux.

   Целостность файлов компонентов проверена.

Результат проверки каждого компонента отображается в следующем формате:

- Блок Summary описывает количество проверенных объектов со статусом проверки: целостность не подтверждена/объект пропущен/целостность подтверждена:
  - Manifests – количество обработанных файлов манифеста.
  - Files – количество обработанных файлов KUMA.
  - Directories – при проверке целостности KUMA не используется.
  - Registries – при проверке целостности KUMA не используется.
  - Registry values – при проверке целостности KUMA не используется.

- Результат проверки целостности компонента:
  - SUCCEEDED – целостность подтверждена.
  - FAILED – целостность нарушена.

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события KUMA. Все события, которые обрабатываются корреляторами KUMA с целью обнаружения алертов, должны соответствовать этой модели. Максимальный размер события, обрабатываемого коллектором KUMA: 4 МБ.

События, несовместимые с этой моделью данных, необходимо преобразовывать в этот формат (нормализовать) с помощью коллекторов.

Модель данных нормализованного события

Название поля	Тип данных	Размер поля	Описание
Назначение данных полей определено в названии поля. Поля доступны для изменения.			
`ApplicationProtocol`	Строка	31 символ	Название протокола прикладного уровня. Например, HTTPS, SSH, Telnet.
`BytesIn`	Число	От -9223372036854775808 до 9223372036854775807	Количество полученных байт.
`BytesOut`	Число	От -9223372036854775808 до 9223372036854775807	Количество отправленных байт.
`DestinationAddress`	Строка	45 символов	IPv4 или IPv6-адрес актива, с которым будет выполнено действие. Например, 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
`DestinationCity`	Строка	1023 символа	Город, соответствующий IP-адресу из поля DestinationAddress.
`DestinationCountry`	Строка	1023 символа	Страна, соответствующая IP-адресу из поля DestinationAddress.
`DestinationDnsDomain`	Строка	255 символов	DNS-часть полного доменного имени точки назначения.
`DestinationHostName`	Строка	1023 символа	Название хоста точки назначения. FQDN точки назначения, если доступно.
`DestinationLatitude`	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля DestinationAddress.
`DestinationLongitude`	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DestinationAddress.
`DestinationMacAddress`	Строка	17 символов	MAC-адрес точки назначения. Например, aa:bb:cc:dd:ee:00
`DestinationNtDomain`	Строка	255 символов	Windows Domain Name точки назначения.
`DestinationPort`	Число	От -9223372036854775808 до 9223372036854775807	Номер порта точки назначения.

DestinationProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса, зарегистрированный на точке назначения.
DestinationProcessName	Строка	1023 символа	Название системного процесса, зарегистрированного на точке назначения. Например, sshd, telnet.
DestinationRegion	Строка	1023 символа	Регион, соответствующий IP-адресу из поля DestinationAddress.
DestinationServiceName	Строка	1023 символа	Название сервиса или службы на стороне точки назначения. Например, sshd.
DestinationTranslatedAddress	Строка	45 символов	IPv4 или IPv6-адрес точки назначения после трансляции. Например. 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DestinationTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на точке назначения после трансляции.
DestinationUserID	Строка	1023 символа	Идентификатор пользователя точки назначения.
DestinationUserName	Строка	1023 символа	Имя пользователя точки назначения.
DestinationUserPrivileges	Строка	1023 символа	Названия ролей, которые идентифицируют пользовательские привилегии точки назначения. Например, User, Guest, Administrator.
DeviceAction	Строка	63 символа	Действие, которое было предпринято источником события. Например, blocked, detected.
DeviceAddress	Строка	45 символов	IPv4 или IPv6-адрес устройства, с которого было получено событие. Например, 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceCity	Строка	1023 символа	Город, соответствующий IP-адресу из поля DeviceAddress.
DeviceCountry	Строка	1023 символа	Страна, соответствующая IP-адресу из поля DeviceAddress.
DeviceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени устройства, с которого было получено событие.
DeviceEventClassID	Строка	1023 символа	Идентификатор типа события, присвоенный источником события.
DeviceExternalID	Строка	255 символов	Идентификатор устройства или приложения, присвоенный источником события. Чтобы поле DeviceExternalID отображалось в виде ссылки в свойствах события, нужно настроить шаблон в правиле обогащения или в правиле корреляции.
DeviceFacility	Строка	1023 символа	Значение параметра facility, установленное источником события.
DeviceHostName	Строка	100 символов	Имя устройства, с которого было получено событие. FQDN устройства, если доступно.
DeviceInboundinterface	Строка	128 символов	Название интерфейса входящего соединения.
DeviceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля DeviceAddress.
DeviceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DeviceAddress
DeviceMacAddress	Строка	17 символов	MAC-адрес устройства, с которого было получено событие. Например, aa:bb:cc:dd:ee:00
DeviceNtDomain	Строка	255 символов	Windows Domain Name устройства.
DeviceOutboundinterface	Строка	128 символов	Название интерфейса исходящего соединения.

DevicePayloadID	Строка	128 символов	Уникальный идентификатор полезной нагрузки (Payload), который ассоциирован с raw-событием.
DeviceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса на устройстве, которое сгенерировало событие.
DeviceProcessName	Строка	1023 символа	Название процесса.
DeviceProduct	Строка	63 символа	Название приложения, сформировавшего событие. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceReceiptTime	Число	От -9223372036854775808 до 9223372036854775807	Время получения события устройством.
DeviceRegion	Строка	1023 символа	Регион, соответствующий IP-адресу из поля DeviceAddress.
DeviceTimeZone	Строка	255 символов	Временная зона устройства, на котором было создано событие.
DeviceTranslatedAddress	Строка	45 символов	Ретранслированный IPv4 или IPv6-адрес устройства, с которого поступило событие. Например, 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceVendor	Строка	63 символа	Название производителя источника события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceVersion	Строка	31 символ	Версия приложения источника события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
EndTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) завершения события.
EventOutcome	Строка	63 символа	Результат выполнения операции. Например, success, failure.
ExternalID	Строка	40 символов	Поле в которое может быть сохранен идентификатор.
FileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания файла.
FileHash	Строка	255 символов	Хеш-сумма файла.
FileID	Строка	1023 символа	Значение идентификатора файла.
FileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения файла.
FileName	Строка	1023 символа	Имя файла, без указания пути к файлу.
FilePath	Строка	1023 символа	Путь к файлу, включая имя файла.
FilePermission	Строка	1023 символа	Список разрешений файла.
FileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер файла.
FileType	Строка	1023 символа	Тип файла.
Message	Строка	1023 символа	Краткое описание события.
Name	Строка	512 символов	Название события.

OldFileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания OLD-файла из события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
OldFileHash	Строка	255 символов	Хеш-сумма OLD-файла.
OldFileID	Строка	1023 символа	Идентификатор OLD-файла.
OldFileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения OLD-файла.
OldFileName	Строка	1023 символа	Имя OLD-файла (без пути).
OldFilePath	Строка	1023 символа	Путь к OLD-файлу, включая имя файла.
OldFilePermission	Строка	1023 символа	Список разрешений OLD-файла.
OldFileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер OLD-файла.
OldFileType	Строка	1023 символа	Тип OLD-файла.
Reason	Строка	1023 символа	Информация о причине возникновения события.
RequestClientApplication	Строка	1023 символа	Значение параметра "user-agent" http-запроса.
RequestContext	Строка	2048 символа	Описание контекста http-запроса.
RequestCookies	Строка	1023 символа	Cookies, связанные с http-запросом.
RequestMethod	Строка	1023 символа	Метод, который использовался при выполнении http-запроса.
RequestUrl	Строка	1023 символа	Запрошенный URL.
Severity	Строка	1023 символа	Приоритет. Это может быть поле Severity или поле Level исходного события.
SourceAddress	Строка	45 символов	IPv4 или IPv6-адрес источника. Пример формата: 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
SourceCity	Строка	1023 символа	Город, соответствующий IP-адресу из поля SourceAddress.
SourceCountry	Строка	1023 символа	Страна, соответствующая IP-адресу из поля SourceAddress.
SourceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени источника.
SourceHostName	Строка	1023 символа	Доменное имя Windows-устройства источника события.
SourceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля SourceAddress.
SourceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля SourceAddress.
SourceMacAddress	Строка	17 символов	MAC-адрес источника. Пример формата: aa:bb:cc:dd:ee:00
SourceNtDomain	Строка	255 символов	Windows Domain Name источника.
SourcePort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта источника.
SourceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса.

SourceProcessName	Строка	1023 символа	Название системного процесса на источнике. Например, sshd, telnet.
SourceRegion	Строка	1023 символа	Регион, соответствующий IP-адресу из поля SourceAddress.
SourceServiceName	Строка	1023 символа	Название сервиса или службы на стороне источника. Например, sshd.
SourceTranslatedAddress	Строка	45 символов	IPv4 или IPv6-адрес источника после трансляции. Пример формата: 0.0.0.0 или xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
SourceTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на источнике после трансляции.
SourceUserID	Строка	1023 символа	Идентификатор пользователя источника.
SourceUserName	Строка	1023 символа	Имя пользователя источника.
SourceUserPrivileges	Строка	1023 символа	Названия ролей, которые идентифицируют пользовательские привилегии источника. Например, User, Guest, Administrator.
StartTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) в которые, началась активность, связанная с событием.
Tactic	Строка	128 символов	Название тактики из матрицы MITRE ATT&CK.
Technique	Строка	128 символов	Название техники из матрицы MITRE ATT&CK.
TransportProtocol	Строка	31 символ	Название протокола Транспортного уровня сетевой модели OSI (например TCP, UDP).
Type	Число	От -9223372036854775808 до 9223372036854775807	Тип события: 1 – базовое, 2 - агрегированное, 3 - корреляционное, 4 - аудит, 5 - мониторинг.
Поля, назначение которых может быть определено пользователем. Поля доступны для изменения.			
DeviceCustomDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
DeviceCustomDate1Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
DeviceCustomDate2Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomDate2.
DeviceCustomFloatingPoint1	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint1Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomFloatingPoint1.
DeviceCustomFloatingPoint2	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint2Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomFloatingPoint2.
DeviceCustomFloatingPoint3	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint3Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomFloatingPoint3.

DeviceCustomFloatingPoint4	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint4Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomFloatingPoint4.
DeviceCustomIPv6Address1	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата: y:y:y:y:y:y:y:y
DeviceCustomIPv6Address1Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomIPv6Address1.
DeviceCustomIPv6Address2	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата: y:y:y:y:y:y:y:y
DeviceCustomIPv6Address2Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomIPv6Address2.
DeviceCustomIPv6Address3	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата: y:y:y:y:y:y:y:y
DeviceCustomIPv6Address3Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomIPv6Address3.
DeviceCustomIPv6Address4	Строка	45 символов	Поле для маппинга значения IPv6 address. Например, y:y:y:y:y:y:y:y
DeviceCustomIPv6Address4Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomIPv6Address4.
DeviceCustomNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber1Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomNumber1.
DeviceCustomNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber2Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomNumber2.
DeviceCustomNumber3	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber3Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomNumber3.
DeviceCustomString1	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString1Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString1.
DeviceCustomString2	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString2Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString2.
DeviceCustomString3	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString3Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString3.
DeviceCustomString4	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString4Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString4.
DeviceCustomString5	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString5Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString5.
DeviceCustomString6	Строка	4000 символов	Поле для маппинга строкового значения.

DeviceCustomString6Label	Строка	1023 символа	Поле для описания назначения поля DeviceCustomString6.
DeviceDirection	Число	От -9223372036854775808 до 9223372036854775807	Поле для описания направления соединения события. "0" - входящее соединение, "1" - исходящее соединение.
DeviceEventCategory	Строка	1023 символа	Категория события, присвоенная устройством, направившим событие в SIEM.
FlexDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FlexDate1Label	Строка	128 символов	Поле для описания назначения поля FlexDate1Label.
FlexNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber1Label	Строка	128 символов	Поле для описания назначения поля FlexNumber1Label.
FlexNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber2Label	Строка	128 символов	Поле для описания назначения поля FlexNumber2Label.
FlexString1	Строка	1023 символа	Поле для маппинга строкового значения.
FlexString1Label	Строка	128 символов	Поле для описания назначения поля FlexString1Label.
FlexString2	Строка	1023 символа	Поле для маппинга строкового значения.
FlexString2Label	Строка	128 символов	Поле для описания назначения поля FlexString2Label.
Служебные поля. Недоступны для редактирования.			
AffectedAssets	Вложенная структура [Affected]	-	Вложенная структура, из которой можно обратиться к связанным с алертом активам и учетным записям, а также узнать, сколько раз они фигурируют в событиях алерта.
AggregationRuleID	Строка	-	Идентификатор правила агрегации.
AggregationRuleName	Строка	-	Название правила агрегации, которое обработало событие.
BaseEventCount	Число	-	Для агрегированного базового события – количество базовых событий, которые были обработаны правилом агрегации. Для корреляционного события – это количество базовых событий, которые были обработаны правилом корреляции, которое создало корреляционное событие.
BaseEvents	Вложенный список [Event]	-	Вложенная структура со списком базовых событий. Поле может быть заполнено у корреляционных событий.
Code	Строка	-	В базовом событии это код возврата процесса, функции или операции из источника.
CorrelationRuleID	Строка	-	ID корреляционного правила.
CorrelationRuleName	Строка	-	Название правила корреляции, в результате срабатывания которого было создано корреляционное событие. Заполняется только для корреляционных событий.
DestinationAccountID	Строка	-	Поле хранит идентификатор пользователя.

`DestinationAssetID`	Строка	-	Поле хранит идентификатор актива точки назначения.
`DeviceAssetID`	Строка	-	Поле хранит идентификатор актива, направившего событие в SIEM.
`Extra`	Вложенный словарь [строка:строка]	-	Поле, в которое во время нормализации сырого события можно поместить те его поля, для которых не настроено сопоставление с полями события KUMA. Это поле может быть заполнено только у базовых событий. Максимальный размер поля – 4 МБ.
`GroupedBy`	Строка	-	Список названия полей, по которым была группировка в правиле корреляции. Заполняется только для корреляционного события.
`ID`	Строка	-	Уникальный идентификатор события типа UUID. Для базового события, генерируемого на коллекторе, идентификатор генерирует коллектор. Идентификатор корреляционного события генерирует коррелятор. Идентификатор никогда не меняет своего значения.
`Raw`	Строка	-	Не нормализованный текст исходного сырого события. Максимальный размер поля – 16 384 байт.
`ReplayID`	Строка	-	Идентификатор ретроспективного сканирования в процессе которого было создано событие.
`ServiceID`	Строка	-	Идентификатор экземпляра сервиса: коррелятора, коллектора, хранилища.
`ServiceName`	Строка	-	Название экземпляра микросервиса, которое присваивает администратор KUMA при создании микросервиса.
`SourceAccountID`	Строка	-	Поле хранит идентификатор пользователя.
`SourceAssetID`	Строка	-	Поле хранит идентификатор актива источника событий.
`SpaceID`	Строка	-	Идентификатор пространства.
`TenantID`	Строка	-	Поле хранит идентификатор тенанта.
`TI`	Вложенный словарь [строка:строка]	-	Поле, в котором в формате словаря содержатся категории, полученные от внешнего источника Threat Intelligence по индикаторам из события.
`Timestamp`	Число	-	Время создания базового события на коллекторе. Время создания корреляционного события на корреляторе. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Value`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Сколько раз актив или учетная запись фигурирует в связанных с алертом событиях.

Поля, формируемые KUMA

KUMA формирует следующие поля, не подлежащие изменениям: BranchID, BranchName, DestinationAccountName, DestinationAssetName, DeviceAssetName, SourceAccountName, SourceAssetName, TenantID (в поле отображается название тенанта – обогащенное значение, при этом для поиска по базе данных используется идентификатор тенанта).

Настройка модели данных нормализованного события из KATA EDR

В ходе расследования инцидентов может оказаться полезной возможность выстроить цепочку процессов. Для этого важно, чтобы идентификаторы процесса KATA/EDR попадали в определенные поля нормализованного события. После корректной настройки нормализации вы можете построить цепочку процессов для событий, поступающих из KATA/EDR, с помощью SQL-запроса.

Пример построения цепочки процессов с помощью SQL-запроса

Пример SQL-запроса для отбора событий, содержащих цепочку процессов

```
SELECT
    b.DeviceHostName AS HostName,
    b.SourceAccountID AS AccountID,
    b.SourceUserName AS UserName,
    a.DeviceCustomString3 AS GrandParentProcessID,
    a.SourceProcessName AS GrandParentProcessName,
    a.DeviceCustomString5 AS ParentProcessID,
    a.DestinationProcessName AS ParentProcessName,
    b.DeviceCustomString5 AS ProcessID,
    b.DestinationProcessName AS ProcessName,
    concat(a.SourceProcessName, ' -> ', a.DestinationProcessName, ' -> ',
b.DestinationProcessName) AS ProcessTree
FROM `events` AS a
INNER JOIN
    (
        SELECT *
        FROM `events`
        WHERE DeviceEventClassID='4688'
    ) AS b
```

```
ON a.DeviceCustomString5 = b.DeviceCustomString3
WHERE DeviceEventClassID='4688'
```

Результат

В результате выполнения запроса в разделе **События** вернутся события, отвечающие условиям запроса. В карточке события в поле `ProcessTree` будет перечислена цепочка процессов process A → process B → ... → process N.

Например:

```
C:\Windows\System32\svchost.exe -> C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.164_none_7e114a3d4d0589d4\TIWorker.exe -> C:\Windows\System32\conhost.exe
```

Для построения цепочки процессов необходимо настроить копирование данных из полей исходных событий в поля нормализованного события в нормализаторах в KUMA следующим образом:

1. Для любых событий KATA/EDR должна быть настроена нормализация с копированием следующих полей:
   - поле события KATA/EDR `EventType` должно копироваться в поле нормализованного события KUMA `DeviceEventCategory`;
   - поле события KATA/EDR `HostName` должно копироваться в поле нормализованного события KUMA `DeviceHostName`.
2. Для любого события, где поле `DeviceProduct = 'KATA'` должна быть настроена нормализация в соответствии с таблицей ниже.

Нормализация полей событий из KATA/EDR

Поле в событии KATA/EDR	Поле нормализованного события
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance
FilePath	FilePath
FileName	FileName
Md5	FileHash
FileSize	FileSize

3. Для событий, перечисленных в таблице ниже, должна быть настроена дополнительная нормализация с копированием полей в соответствии с таблицей.

Дополнительная нормализация с копированием полей событий из KATA/EDR

Событие	Поле исходного события	Поле нормализованного события
Process	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName

Событие	Поле исходного события	Поле нормализованного события
AppLock	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Module	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Driver	HostName	DeviceHostName
	FileName	FileName
	ProductName	DeviceCustomString5,
		ProductName
	ProductVendor	DeviceCustomString6
		ProductVendor
Connection	UniquePid	FlexString2
	HostName	DeviceHostName
	URI	RequestURL
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	HostName	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort

Событие	Поле исходного события	Поле нормализованного события
Registry	UniquePid	FlexString2
	HostName	DeviceHostName
	ValueName	DeviceCustomString5
		New Value Name
	KeyName	DeviceCustomString4
		New Key Name
	PreviousKeyName	FlexString2
		Old Key Name
	ValueData	DeviceCustomString6
		New Value Data
	PreviousValueData	FlexString1
		Old Value Data
	ValueType	FlexNumber1
		Value Type
	PreviousValueType	FlexNumber2
		Previous Value Type
SystemEventLog	UniquePid	FlexString2
	HostName	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID
ThreatDetect	UniquePid	FlexString2
	HostName	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		Is Silent
	RecordId	DeviceCustomString5
		Record ID
	DatabaseTimestamp	DeviceCustomDate2
		Database Timestamp
ThreatDetectProcessingResult	UniquePid	FlexString2
	HostName	DeviceHostName
	ThreatStatus	DeviceCustomString5
		Threat Status

Событие	Поле исходного события	Поле нормализованного события
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize
	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	HostName	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		Command Line
AMSI SCAN	UniquePid	FlexString2
	HostName	DeviceHostName
	ObjectContent	DeviceCustomString5
		Object Content

Модель данных алерта

В этом разделе описана модель данных алерта KUMA. Алерты создаются корреляторами при выявлении с помощью правил корреляции угроз безопасности информации. Алерты необходимо расследовать для устранения этих угроз.

Поле алерта	Тип данных	Описание
`ID`	Строка	Уникальный идентификатор алерта.
`TenantID`	Строка	Идентификатор тенанта, которому принадлежит алерт. Значение наследуется от коррелятора, создавшего алерт.
`TenantName`	Строка	Название тенанта.
`CorrelationRuleID`	Строка	Идентификатор правила, на основании которого был создан алерт.
`CorrelationRuleName`	Строка	Название правила корреляции, на основании которого был создан алерт.
`Status`	Строка	Статус алерта. Возможные значения: • `New` – новый алерт. • `Assigned` – алерт назначен пользователю. • `Closed` – алерт закрыт. • `Exported to IRP` – алерт выгружен IRP-систему для дальнейшего расследования. • `Escalated` – на основе алерта создан инцидент.
`Priority`	Число	Уровень важности алерта. Возможные значения: • 1–4 – Низкий. • 5–8 – Средний. • 9–12 – Высокий. • 13–16 – Критический.
`ManualPriority`	Строка `TRUE/FALSE`	Параметр, показывающий, как был определен уровень важности алерта. Возможные значения: • `true` – задан пользователем. • `false` (значение по умолчанию) – рассчитан автоматически.
`FirstSeen`	Число	Время создания первого корреляционного события из алерта.
`LastSeen`	Число	Время создания последнего корреляционного события из алерта.

`UpdatedAt`	Число	Дата последнего изменения параметров алерта.
`UserID`	Строка	Идентификатор пользователя KUMA, которому алерт назначен на рассмотрение.
`UserName`	Строка	Имя пользователя KUMA, которому алерт назначен на рассмотрение.
`GroupedBy`	Вложенный список строк	Перечень полей событий, по которым группировались событий в правиле корреляции.
`ClosingReason`	Строка	Причина закрытия алерта. Возможные значения: • `Incorrect Correlation Rule` – алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции. • `Incorrect Data` – алерт был ложным, а полученные события не указывают на угрозу безопасности. • `Responded` – были приняты необходимые меры по устранению угрозы безопасности.
`MaxAssetsWeightStr`	Строка	Максимальный уровень важности категорий активов, связанных с алертом.
`MaxAssetCategoryImportance`	Строка	Поле содержит значение поля `MaxAssetsWeightStr` в формате, удобном для отображения. Возможные значения: • `Unknown` • `Low` • `Medium` • `High` • `Critical`
`IntegrationID`	Строка	Идентификатор алерта в программе IRP / SOAR, если в KUMA настроена интеграция с такой программой.
`ExternalReference`	Строка	Ссылка на раздел в программе IRP / SOAR, в котором отображаются сведения об импортированном из KUMA алерте.
`IncidentID`	Строка	Идентификатор инцидента, к которому привязан алерт.
`IncidentName`	Строка	Название инцидента, к которому привязан алерт.
`SegmentationRuleName`	Строка	Название правила сегментации, по которому корреляционные события сгруппированы в алерте.
`BranchID`	Строка	Идентификатор ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`BranchName`	Строка	Название ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`Actions`	Вложенная структура `[Action]`	Вложенная структура со строками, в которых указаны изменения статусов и назначений алерта, пользовательские комментарии.
`Events`	Вложенная структура `[EventWrapper]`	Вложенная структура, из которой можно обратиться к связанным с алертом корреляционным событиям.
`Assets`	Вложенная структура `[Asset]`	Вложенная структура, из которой можно обратиться к связанным с алертом активам.
`Accounts`	Вложенная структура `[Account]`	Вложенная структура, из которой можно обратиться к связанным с алертом учетным записям.
`AffectedAssets`	Вложенная структура `[Affected]`	Вложенная структура, из которой можно обратиться к связанным с алертам активам и учетным записям, а также узнать, сколько раз они фигурируют в событиях алерта.

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Value`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Вложенная структура `EventWrapper`

Поле	Тип данных	Описание
`Event`	Вложенная структура `[Event]`	Поля события.
`Comment`	Строка	Комментарий, добавленный при добавлении событий к алерту.
`LinkedAt`	Число	Дата добавления событий к алерту.

Вложенная структура `Action`

Поле	Тип данных	Описание
`CreatedAt`	Число	Дата, когда действие над алертом было произведено.
`UserID`	Строка	Идентификатор пользователя.
`Kind`	Строка	Тип действия.
`Value`	Строка	Значение.
`Event`	Вложенная структура `[Event]`	Поля события.
`ClusterID`	Строка	Идентификатор кластера.

Модель данных актива

Структура актива представлена полями, в которых содержатся значения. Поля также могут содержать вложенные структуры.

Поле актива	Тип значения	Описание
`ID`	Строка	Идентификатор актива.
`TenantName`	Строка	Название тенанта.
`DeletedAt`	Число	Дата удаления актива.
`CreatedAt`	Число	Дата создания актива.
`TenantID`	Строка	Идентификатор тенанта.
`DirectCategories`	Вложенный список строк	Категории актива.
`CategoryModels`	Вложенная структура `[Category]`	Изменение категорий актива.

AffectedByIncidents	Вложенный словарь: [строка:строка TRUE/FALSE]	Идентификаторы инцидентов.
IPAddress	Вложенный список строк	IP-адреса актива.
FQDN	Строка	FQDN актива.
Weight	Число	Уровень важности актива.
Deleted	Строка со значениями TRUE/FALSE	Помечен ли актив на удаление из KUMA.
UpdatedAt	Число	Дата последнего обновления актива.
MACAddress	Вложенный список строк	MAC-адреса актива.
IPAddressInt	Вложенный список чисел	IP-адрес в виде числа.
Owner	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
OS	Вложенная структура [OS]	Сведения об операционной системы актива.
DisplayName	Строка	Название актива.
APISoft	Вложенная структура [Software]	ПО, установленное на активе.
APIVulns	Вложенная структура [Vulnerability]	Уязвимости актива.
KICSServerIp	Строка	IP-адрес сервера KICS/KATA.
KICSConnectorID	Число	Идентификатор коннектора KICS/KATA.
KICSDeviceID	Число	Идентификатор актива в KICS/KATA.
KICSStatus	Строка	Статус актива в KICS/KATA.
KICSHardware	Вложенная структура [KICSSystemInfo]	Аппаратные сведения об активе, полученные из KICS/KATA.
KICSSoft	Вложенная структура [KICSSystemInfo]	Сведения о ПО актива, полученные из KICS/KATA.
KICSRisks	Вложенная структура [KICSRisk]	Сведения об уязвимостях актива, полученные из KICS/KATA.
Sources	Вложенная структура [Sources]	Основные сведения об активе, поступавшие из разных источников.
FromKSC	Строка со значениями TRUE/FALSE	Индикатор, указывающий, что сведения об активе импортированы из KSC.
NAgentID	Строка	Идентификатор агента KSC, от которого получены сведения об активе.
KSCServerFQDN	Строка	FQDN сервера KSC.
KSCInstanceID	Строка	Идентификатор экземпляра KSC.
KSCMasterHostname	Строка	Имя хоста сервера KSC.
KSCGroupID	Число	Идентификатор группы KSC.
KSCGroupName	Строка	Название группы KSC.
LastVisible	Число	Дата, когда от KSC в последний раз были получены сведения об активе.
Products	Вложенный словарь: [строка:вложенная структура [ProductInfo]]	Сведения об установленных на активе приложениях Kaspersky, полученные из KSC.
Hardware	Вложенная структура [Hardware]	Аппаратные сведения об активе, полученные из KSC.
KSCSoft	Вложенная структура [Software]	Сведения о ПО актива, полученные из KSC.
KSCVulns	Вложенная структура [Vulnerability]	Сведения об уязвимостях актива, полученные из KSC.

Вложенная структура `Category`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор категории.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`Parent`	Строка	Родительская категория.
`Path`	Вложенный список строк	Структура категорий.
`Name`	Строка	Название категории.
`UpdatedAt`	Число	Последнее обновление категории.
`CreatedAt`	Число	Дата создания категории.
`Description`	Строка	Описание категории.
`Weight`	Число	Уровень важности категории.
`CategorizationKind`	Строка	Тип присвоения категории активам.
`CategorizationAt`	Число	Дата категоризации.
`CategorizationInterval`	Строка	Интервал присвоения категорий.

Вложенная структура `OwnerInfo`

Поле	Тип значения	Описание
`DisplayName`	Строка	Имя владельца актива.

Вложенная структура `OS`

Поле	Тип значения	Описание
`Name`	Строка	Название операционной системы.
`BuildNumber`	Число	Версия операционной системы.

Вложенная структура `Software`

Поле	Тип значения	Описание
`DisplayName`	Строка	Название ПО.
`DisplayVersion`	Строка	Версия ПО.
`Publisher`	Строка	Издатель ПО.

`InstallDate`	Строка	Дата установки.
`HasMSIInstaller`	Строка `TRUE/FALSE`	Признак, имеет ли ПО MSI-установщик.

Вложенная структура `Vulnerability`

Поле	Тип значения	Описание
`KasperskyID`	Строка	Идентификатор уязвимости, присвоенный Kaspersky.
`ProductName`	Строка	Название ПО.
`DescriptionURL`	Строка	URL с описанием уязвимости.
`RecommendedMajorPatch`	Строка	Рекомендуемое обновление.
`RecommendedMinorPatch`	Строка	Рекомендуемое обновление.
`SeverityStr`	Строка	Уровень важности уязвимости.
`Severity`	Число	Уровень важности уязвимости.
`CVE`	Вложенный список строк	Идентификатор уязвимости CVE.
`ExploitExists`	Строка `TRUE/FALSE`	Существует ли эксплойт.
`MalwareExists`	Строка `TRUE/FALSE`	Существует ли вредоносная программа.

Вложенная структура `KICSSystemInfo`

Поле	Тип значения	Описание
`Model`	Строка	Модель устройства.
`Version`	Строка	Версия устройства.
`Vendor`	Строка	Производитель.

Вложенная структура `KICSRisk`

Поле	Тип значения	Описание
`ID`	Число	Идентификатор риска KICS/KATA.
`Name`	Строка	Название риска.
`Category`	Строка	Тип риска.
`Description`	Строка	Описание риска.
`DescriptionUrl`	Строка	Ссылка на описание риска.
`Severity`	Число	Уровень важности риска.
`Cvss`	Число	Оценка CVSS.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`KSC`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KSC.
`API`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие через REST API.
`Manual`	Вложенная структура `[SourceInfo]`	Сведения об активе, введенные вручную.
`KICS`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KICS /KATA.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура `[OwnerInfo]`	Сведения о владельце актива.
`OS`	Вложенная структура `[OS]`	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.

Вложенная структура `ProductInfo`

Поле	Тип значения	Описание
`ProductVersion`	Строка	Версия ПО.
`ProductName`	Строка	Название ПО.

Вложенная структура `Hardware`

Поле	Тип значения	Описание
`NetCards`	Вложенная структура `[NetCard]`	Перечень сетевых карт актива.
`CPU`	Вложенная структура `[CPU]`	Перечень процессоров актива.
`RAM`	Вложенная структура `[RAM]`	Перечень ОЗУ актива.
`Disk`	Вложенная структура `[Disk]`	Перечень дисков актива.

Вложенная структура `NetCard`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор сетевой карты.
`MACAddresses`	Вложенный список строк	MAC-адреса сетевой карты.
`Name`	Строка	Название сетевой карты.
`Manufacture`	Строка	Производитель сетевой карты.
`DriverVersion`	Строка	Версия драйвера.

Вложенная структура `RAM`

Поле	Тип значения	Описание
`Frequency`	Строка	Частота ОЗУ.
`TotalBytes`	Число	Объем ОЗУ в байтах.

Вложенная структура `CPU`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор процессора.
`Name`	Строка	Название процессора.
`CoreCount`	Строка	Количество ядер.
`CoreSpeed`	Строка	Частота.

Вложенная структура `Disk`

Поле	Тип значения	Описание
`FreeBytes`	Число	Свободное пространство на диске.
`TotalBytes`	Число	Общее пространство на диске.

Модель данных учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты, а также при корреляции событий.

Поле	Тип значения	Описание
ID	Строка	Идентификатор учетной записи.
ObjectGUID	Строка	Атрибут Active Directory. Идентификатор учетной записи в Active Directory.
TenantID	Строка	Идентификатор тенанта.
TenantName	Строка	Название тенанта.
UpdatedAt	Число	Последнее обновление учетной записи.
Domain	Строка	Домен.
CN	Строка	Атрибут Active Directory. Имя пользователя.
DisplayName	Строка	Атрибут Active Directory. Отображаемое имя пользователя.
DistinguishedName	Строка	Атрибут Active Directory. Название объекта LDAP.
EmployeeID	Строка	Атрибут Active Directory. Идентификатор сотрудника.
Mail	Строка	Атрибут Active Directory. Электронная почта пользователя.
MailNickname	Строка	Атрибут Active Directory. Альтернативный адрес электронной почты.
Mobile	Строка	Атрибут Active Directory. Номер мобильного телефона.
ObjectSID	Строка	Атрибут Active Directory. Идентификатор безопасности.
SAMAccountName	Строка	Атрибут Active Directory. Логин.
TelephoneNumber	Строка	Атрибут Active Directory. Номер телефона.
UserPrincipalName	Строка	Атрибут Active Directory. Имя участника-пользователя.
Archived	Строка TRUE/FALSE	Признак, определяющий, является ли учетная запись устаревшей.
MemberOf	Список строк	Атрибут Active Directory. Группы AD, в которые внесен пользователь. По этому атрибуту события можно искать при корреляции.
PreliminarilyArchived	Строка TRUE/FALSE	Признак, определяющий, требуется ли обозначить учетную запись как устаревшую.
CreatedAt	Число	Дата создания учетной записи.
SN	Строка	Атрибут Active Directory. Фамилия пользователя.
SAMAccountType	Строка	Атрибут Active Directory. Тип учетной записи.
Title	Строка	Атрибут Active Directory. Должность пользователя.
Division	Строка	Атрибут Active Directory. Подразделение пользователя.
Department	Строка	Атрибут Active Directory. Отдел пользователя.
Manager	Строка	Атрибут Active Directory. Руководитель пользователя.
Location	Строка	Атрибут Active Directory. Местоположение пользователя.
Company	Строка	Атрибут Active Directory. Компания пользователя.
StreetAddress	Строка	Атрибут Active Directory. Адрес компании.
PhysicalDeliveryOfficeName	Строка	Атрибут Active Directory. Адрес для доставки.
ManagedObjects	Список строк	Атрибут Active Directory. Объекты, находящиеся под управлением пользователя.
UserAccountControl	Число	Атрибут Active Directory. Тип учетной записи AD.
WhenCreated	Число	Атрибут Active Directory. Дата создания учетной записи.
WhenChanged	Число	Атрибут Active Directory. Дата изменения учетной записи.
AccountExpires	Число	Атрибут Active Directory. Дата истечения срока учетной записи.
BadPasswordTime	Число	Атрибут Active Directory. Дата последней неудачной попытки входа в систему.

События аудита KUMA

События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью, и используются для обеспечения целостности системы.

События аудита создаются на сервере Ядра KUMA и отправляются в хранилища тенанта Main и корреляторы тенанта Main. Поэтому для хранения событий аудита должно быть создано хотя бы одно хранилище в тенанте Main. Если хранилища нет, вам нужно создать его. События аудита отправляются в пространство KUMA Audit, которое создается автоматически внутри хранилища.

Чтобы просмотреть события аудита, вам нужно перейти в раздел KUMA **События** и добавить в запрос `SELECT * FROM 'events' WHERE Type=4`.

В результате выполнения запроса отобразятся события аудита, если роль пользователя предусматривает права для просмотра событий аудита.

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные в таблице ниже.

Название поля события	Значение поля
`Timestamp`	Время события.
`DeviceHostName`	Хост источника события. Для событий аудита указывается имя хоста, на котором установлена служба kuma-core, потому что она является источником событий.
`DeviceTimeZone`	Часовой пояс системного времени сервера, на котором установлено Ядро KUMA в формате `+-чч:мм`.
`Type`	Тип события аудита. `Audit` или `Base`.
`TenantID`	Идентификатор тенанта.
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`EndTime`	Время создания события.
`SpaceID`	`KUMA Audit`
`DeviceAction`	Действие, которое зафиксировано в событии аудита.

Пользователь успешно вошел в систему или не смог войти

Название поля события	Значение поля
`DeviceAction`	`user login`
`EventOutcome`	`succeeded` или `failed`
`SourceTranslatedAddress`	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
`SourceAddress`	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.

SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.
Message	Описание ошибки. Появляется только в том случае, если при входе в систему произошла ошибка. В противном случае поле будет пустым.

Логин пользователя изменен

Название поля события	Значение поля
DeviceAction	user login changed
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение логина.
DeviceCustomString1Label	new login
DeviceCustomString2	Значение логина до его изменения.
DeviceCustomString2Label	old login

Другие данные пользователя изменены

Название поля события	Значение поля
DeviceAction	user other info changed
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.

Пользователь вышел из системы

Это событие создается только тогда, когда пользователь нажимает кнопку выхода.

Это событие не создается, если пользователь покидает систему из-за окончания сеанса или если пользователь снова входит в систему из другого браузера.

Значения полей события аудита Пользователь вышел из системы

Название поля события	Значение поля
DeviceAction	user logout
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.

Пароль пользователя изменен

Название поля события	Значение поля
DeviceAction	user password changed
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.

Пользователь создан

Название поля события	Значение поля
DeviceAction	user created
EventOutcome	succeeded

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который создал учетную запись.
SourceUserID	Идентификатор пользователя, который создал учетную запись.
DestinationUserName	Логин пользователя, для которого была создана учетная запись.
DestinationUserID	Идентификатор пользователя, для которого была создана учетная запись.
DeviceCustomString1	Роль созданного пользователя.
DeviceCustomString1Label	`role`

Пользователю назначена роль

Название поля события	Значение поля
DeviceAction	`granted access`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, данные которого изменены.
SourceUserID	Идентификатор пользователя, данные которого изменены.
DestinationUserPrivileges	Идентификатор роли пользователя, данные которого изменены.
DeviceCustomString5	Идентификатор тенанта, который использовался, чтобы назначить роль.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Роль пользователя отозвана

Название поля события	Значение поля
DeviceAction	`revoked access`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

SourceUserName	Логин пользователя, который внес изменения.
SourceUserID	Идентификатор пользователя, который внес изменения.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.
DestinationUserPrivileges	Идентификатор роли пользователя, данные которого были изменены.
DeviceCustomString5	Идентификатор тенанта, который использовался, чтобы назначить роль.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Пользователь изменил параметры набора полей для определения источников

Название поля события	Значение поля
DeviceAction	settings updated
DeviceFacility	eventSourceIdentity
EventOutcome	succeeded
SourceUserName	Логин пользователя, который внес изменения.
SourceUserID	Идентификатор пользователя, который внес изменения.
DeviceCustomString5	Обновленный набор полей, | используется в качестве разделителя.

Пользователю назначен алерт

Название поля события	Значение поля
DeviceAction	user is assigned to alert
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который назначил алерт пользователю.
SourceUserID	Идентификатор пользователя, который назначил алерт пользователю.
ExternalID	Идентификатор алерта.
Name	Имя алерта.
DestinationUserName	Логин пользователя, которому назначили алерт.
DestinationUserID	Идентификатор пользователя, которому назначили алерт.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Токен доступа пользователя изменен

Название поля события	Значение поля
DeviceAction	user access token changed
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.

Добавлен файл ключа

Название поля события	Значение поля
DeviceAction	license key installed
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа.
SourceUserName	Логин пользователя, который добавил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Приложение активировано с помощью кода активации

Название поля события	Значение поля
DeviceAction	license activated
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который указал код активации.

SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Резервный лицензионный ключ добавлен

Название поля события	Значение поля
DeviceAction	`reserve license key installed`
DeviceAddress	IP-адрес устройства, на котором добавлен резервный лицензионный ключ.
EventOutcome	`succeeded`
Message	Название лицензии.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который добавил резервный лицензионный ключ.
SourceUserName	Логин пользователя, который добавил резервный лицензионный ключ.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Резервный лицензионный ключ удален

Название поля события	Значение поля
DeviceAction	`reserve license key uninstalled`
DeviceAddress	IP-адрес устройства, на котором удален резервный лицензионный ключ.
EventOutcome	`succeeded`
Message	Название лицензии.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который удалил резервный лицензионный ключ.
SourceUserName	Логин пользователя, который удалил резервный лицензионный ключ.

DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Срок действия лицензии продлен

Название поля события	Значение поля
DeviceAction	license reactivated
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа.
SourceUserName	Логин пользователя, который добавил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Недействительный код активации

Название поля события	Значение поля
DeviceAction	activation code license activated
EventOutcome	failed
Message	Текст ошибки.
SourceUserID	Идентификатор пользователя, который указал код активации.
SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Код активации заблокирован

Название поля события	Значение поля
DeviceAction	Activation code blocked
EventOutcome	succeeded
Message	Название лицензии.

SourceUserID	Идентификатор пользователя, который указал код активации.
SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Код активации или файл ключа удален

Название поля события	Значение поля
DeviceAction	`Activation code or key file uninstalled`
EventOutcome	`succeeded`
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который удалил файл ключа.
SourceUserName	Логин пользователя, который удалил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Код активации или файл ключа заменен

Название поля события	Значение поля
DeviceAction	`Activation code or key file replaced`
EventOutcome	`succeeded`
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который выполнил замену.
SourceUserName	Логин пользователя, который выполнил замену.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Превышено количество EPS

Название поля события	Значение поля
DeviceAction	license limit for EPS exceeded
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Окончание срока действия лицензии и начало льготного периода

Название поля события	Значение поля
DeviceAction	license expired
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Окончание льготного периода

Название поля события	Значение поля
DeviceAction	license ended
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Добавлен код активации или файл ключа с истекшим сроком годности

Название поля события	Значение поля
DeviceAction	`Activation code or key file installed`
IP	IP-адрес, на котором добавлен файл ключа или указан код активации.
EventOutcome	`failed`
Message	Текст ошибки.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Изменен набор пространств для разграничения доступа к событиям

Название поля события	Значение поля
DeviceAction	• `space set was created` • `space set was deleted` • `space set was updated` (включая выдачу прав доступа и отзыв прав доступа)
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.

DeviceCustomString5	Идентификатор набора пространств.
DeviceCustomString5Label	set ID
DeviceCustomString3	Название набора пространств.
DeviceCustomString3Label	space name

Изменены пороговые значения для мониторинга сервисов

Название поля события	Значение поля
DeviceAction	settings updated
DeviceFacility	serviceAlertSettings
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.
DeviceCustomString1	JSON с пороговыми значениями, записанными в базе данных.
DeviceCustomString1Label	thresholds
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Изменены значения параметров Ядра KUMA

Название поля события	Значение поля
DeviceAction	settings updated
DeviceFacility	coreProperties
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.
DeviceCustomString1	JSON со значениями параметров Ядра KUMA, записанными в базе данных.
DeviceCustomString1Label	properties

Базы GeoIP импортированы

Название поля события	Значение поля
DeviceAction	new geobase imported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который импортировал базы.
SourceUserID	Идентификатор пользователя, который импортировал базы.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис создан

Название поля события	Значение поля
DeviceAction	service created
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который создал сервис.
SourceUserID	Идентификатор пользователя, который создал сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис удален

Название поля события	Значение поля
DeviceAction	service deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который удалил сервис.
SourceUserID	Идентификатор пользователя, который удалил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DestinationHostName	Полное доменное имя компьютера, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис перезагружен

Название поля события	Значение поля
DeviceAction	service reloaded
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который перезагрузил сервис.
SourceUserID	Идентификатор пользователя, который перезагрузил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.

DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис перезапущен

Название поля события	Значение поля
DeviceAction	service restarted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который перезапустил сервис.
SourceUserID	Идентификатор пользователя, который перезапустил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис запущен

Название поля события	Значение поля
DeviceAction	service started
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, на котором был запущен сервис.
DestinationHostName	Полное доменное имя устройства, на котором был запущен сервис.
DeviceCustomString5	Идентификатор тенанта.

DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис сопряжен

Название поля события	Значение поля
DeviceAction	service paired
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Статус сервиса изменен

Название поля события	Значение поля
DeviceAction	service status changed
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, на котором был запущен сервис.
DestinationHostName	Полное доменное имя устройства, на котором был запущен сервис.
DeviceCustomString1	green, yellow или red
DeviceCustomString1Label	new status
DeviceCustomString2	green, yellow или red
DeviceCustomString2Label	old status
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Партиция удалена пользователем

Название поля события	Значение поля
DeviceAction	partition deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который удалил партицию.
SourceUserID	Идентификатор пользователя, который удалил партицию.
Name	Название хранилища | Тенант перемещаемой или удаляемой партиции | Название пространства, которому принадлежит партиция.
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце `date`.
DeviceCustomDate1Label	date of event
Message	deleted by user

Партиция удалена автоматически по истечении срока хранения

Название поля события	Значение поля
DeviceAction	partition deleted
EventOutcome	succeeded
Name	Название пространства, которому принадлежит партиция.
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of event
SourceServiceName	scheduler
Message	deleted by retention period settings

Удаление партиции по абсолютному сроку хранения

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	deleted partition data
DeviceAction	applied retention policy by GB
SourceServiceName	scheduler

DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Удаление партиции по относительному сроку хранения

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	deleted partition data
DeviceAction	applied retention policy by percent
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Перемещение партиции в холодное хранилище

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	moved partition data to cold storage
DeviceAction	Доступны следующие значения: • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events

EventOutcome	succeeded
DeviceCustomString1	Идентификатор пространства.
DeviceCustomString1Label	nodeID

Перемещение партиции в холодное хранилище завершилось с ошибкой

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	move partition data to cold storage failed: {"error":"Code: 243. DB::Exception: Move is not possible. Not enough space on 'cold_volume'. (NOT_ENOUGH_SPACE) (version 23.8.8.207)\n"}
DeviceAction	Доступны следующие значения: • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	failed
DeviceCustomString1	Идентификатор пространства.
DeviceCustomString1Label	nodeID

Активный лист успешно очищен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что активный лист может быть очищен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли очищен активный лист.

Значения полей события аудита Активный лист успешно очищен или операция завершилась с ошибкой

Название поля события	Значение поля
`DeviceAction`	`active list cleared`
`EventOutcome`	`succeeded` или `failed`
`SourceTranslatedAddress`	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
`SourceAddress`	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
`SourcePort`	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
`SourceUserName`	Логин пользователя, который использовался для очистки активного листа.
`SourceUserID`	Идентификатор пользователя, который использовался для очистки активного листа.
`DeviceExternalID`	Идентификатор сервиса, активные лист которого был очищен.
`ExternalID`	Идентификатор активного листа.
`Name`	Название активного листа.
`Message`	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
`DeviceCustomString5`	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
`DeviceCustomString5Label`	tenant ID
`DeviceCustomString6`	Название тенанта.
`DeviceCustomString6Label`	tenant name

Элемент активного листа успешно изменен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на изменение элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до изменения или после изменения.

Это означает, что элемент активного листа может быть изменен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли изменен элемент активного листа.

Значения полей события аудита Элемент активного листа успешно изменен или операция завершилась с ошибкой

Название поля события	Значение поля
`DeviceAction`	`active list item changed`

EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для изменения элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был изменен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	название тенанта
DeviceCustomString6Label	tenant name

Элемент активного листа успешно удален или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус succeeded или failed.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус failed, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли удален элемент активного листа.

Значения полей события аудита Элемент активного листа успешно удален или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	active list item deleted
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для удаления элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для удаления элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Активный лист успешно импортирован или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Импорт элементов активного листа выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Значения полей события аудита Активный лист успешно импортирован или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	active list imported
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.

DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке. Текст ошибки может быть в формате json, например `{"error":"line 1: header does not contain column IP!"}`.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	название тенанта
DeviceCustomString6Label	tenant name

Активный лист экспортирован

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Значения полей события аудита Активный лист экспортирован

Название поля события	Значение поля
DeviceAction	active list exported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	название тенанта
DeviceCustomString6Label	tenant name

Контекстная таблица экспортирована

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Значения полей события аудита Контекстная таблица экспортирована

Название поля события	Значение поля
DeviceAction	context table exported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Контекстная таблица успешно импортирована или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Импорт элементов контекстной таблицы выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Значения полей события аудита Контекстная таблица успешно импортирована или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table imported
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор контекстной таблицы.

Name	Название контекстной таблицы.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус succeeded или failed.

Параметры события аудита Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table item is set
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для изменения элемента контекстной таблицы.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента контекстной таблицы.
DeviceExternalID	Идентификатор сервиса, контекстная таблица которого была изменена.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
DeviceCustomString1	Название ключа записи.
DeviceCustomString1Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус `succeeded` или `failed`.

Значения полей события аудита Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой

Название поля события	Значение поля
`DeviceAction`	`context table item deleted`
`EventOutcome`	`succeeded` или `failed`
`SourceTranslatedAddress`	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
`SourceAddress`	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
`SourcePort`	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
`SourceUserName`	Логин пользователя, который использовался для удаления элемента контекстной таблицы.
`SourceUserID`	Идентификатор пользователя, который использовался для удаления элемента контекстной таблицы.
`DeviceExternalID`	Идентификатор сервиса, для которого происходит удаление элемента контекстной таблицы.
`ExternalID`	Идентификатор контекстной таблицы.
`Name`	Название контекстной таблицы.
`DeviceCustomString1`	Название ключа записи.
`DeviceCustomString1Label`	`key`
`Message`	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
`DeviceCustomString5`	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Название тенанта.
`DeviceCustomString6Label`	`tenant name`

Контекстная таблица успешно очищена или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на очистку контекстной таблицы осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что контекстная таблица может быть очищена успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, была ли очищена контекстная таблица.

Значения полей события аудита Контекстная таблица успешно очищена или операция завершилась с ошибкой

Название поля события	Значение поля
`DeviceAction`	`context table cleared`
`EventOutcome`	`succeeded` или `failed`
`SourceTranslatedAddress`	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для очистки контекстной таблицы.
SourceUserID	Идентификатор пользователя, который использовался для очистки контекстной таблицы.
DeviceExternalID	Идентификатор сервиса, контекстная таблица которого была очищена.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс добавлен

Название поля события	Значение поля
DeviceAction	`resource added`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для добавления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для добавления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс удален

Название поля события	Значение поля
DeviceAction	resource deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для удаления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для удаления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс обновлен

Название поля события	Значение поля
DeviceAction	resource updated
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для обновления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для обновления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Импорт ресурсов

Название поля события	Значение поля
DeviceAction	import resources
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который импортировал ресурсы.
SourceUserID	Идентификатор пользователя, который импортировал ресурсы.
DeviceCustomString5	Идентификатор тенанта, в который импортировали ресурсы.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта, в который импортировали ресурсы.
DeviceCustomString6Label	tenant name
FileType	Источник импорта: file или repository.
FileID	Если ресурсы импортированы из репозитория, идентификатор пакета. Если ресурсы импортированы из файла, системный идентификатор файла.
ExternalID	Если ресурсы импортированы из репозитория, версия импортированного пакета. Если ресурсы импортированы из файла, пустое значение.

Актив создан

Название поля события	Значение поля
DeviceAction	asset created
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceAssetID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	addresses
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Актив удален

Название поля события	Значение поля
DeviceAction	asset deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceAssetID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	addresses

DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Категория актива добавлена

Название поля события	Значение поля
DeviceAction	category created
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для добавления категории.
SourceUserID	Идентификатор пользователя, который использовался для добавления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Категория актива удалена

Название поля события	Значение поля
DeviceAction	category deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для удаления категории.
SourceUserID	Идентификатор пользователя, который использовался для удаления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Параметры обновлены

Название поля события	Значение поля
DeviceAction	settings updated
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для обновления параметров.
SourceUserID	Идентификатор пользователя, который использовался для обновления параметров.
DeviceFacility	Тип параметров.
DeviceCustomString1	JSON с пороговыми значениями, записанными в базу данных.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Тенант создан

Название поля события	Значение поля
DeviceAction	tenant created
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для создания тенанта.
SourceUserID	Идентификатор пользователя, который использовался для создания тенанта.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Тенант включен

Название поля события	Значение поля
DeviceAction	tenant enabled
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для включения тенанта.
SourceUserID	Идентификатор пользователя, который использовался для включения тенанта.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Тенант выключен

Название поля события	Значение поля
DeviceAction	tenant disabled
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для выключения тенанта.
SourceUserID	Идентификатор пользователя, который использовался для выключения тенанта.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Другие данные тенанта изменены

Название поля события	Значение поля
DeviceAction	tenant other info changed

EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных тенанта.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных тенанта.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Словарь успешно обновлен на сервисе или операция завершилась ошибкой

Название поля события	Значение поля
DeviceAction	dictionary update succeeded
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	Идентификатор сервиса.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	dictionary type
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.

Запись добавлена в словарь

Выполнено добавление или обновление записи в словаре через API.

Значения полей события аудита Запись добавлена в словарь

Название поля события	Значение поля
DeviceAction	dictionary item added
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который добавил запись.
SourceUserID	Идентификатор пользователя, который добавил запись.
DeviceExternalID	Идентификатор сервиса.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	dictionary type
DeviceCustomString2	Ключ записи.
DeviceCustomString2Label	key
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Запись успешно удалена из словаря или операция завершилась с ошибкой

Выполнено удаление записи из словаря (для типов: таблица, словарь) через API.

Событию может быть присвоен статус `succeeded` или `failed`.

Значения полей события аудита Запись успешно удалена из словаря или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	dictionary item deleted
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который удалял запись из словаря.
SourceUserID	Идентификатор пользователя, который удалял запись из словаря.
DeviceExternalID	Идентификатор сервиса, запись в словаре которого была удалена.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	dictionary type
DeviceCustomString2	Ключ записи.
DeviceCustomString2Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Инцидент успешно создан или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	incident created
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который создал инцидент.
SourceUserID	Идентификатор пользователя, который создал инцидент.
ExternalID	Идентификатор инцидента.
Name	Имя инцидента.
DeviceCustomString1	Имя алерта. Поле заполняется, если инцидент создан на основе алерта. Если алертов несколько, имена алертов будут указаны через запятую.
DeviceCustomString1Label	alert name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Инцидент успешно закрыт или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	incident closed
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который закрыл инцидент.
SourceUserID	Идентификатор пользователя, который закрыл инцидент.
ExternalID	Идентификатор инцидента.
Name	Имя инцидента.
DeviceCustomString1	Решение: подтвержден или не подтвержден.
DeviceCustomString1Label	resolution
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Пользователю назначен инцидент или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	user is assigned to incident
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который назначил пользователя.
SourceUserID	Идентификатор пользователя, который назначил пользователя.
ExternalID	Идентификатор инцидента.

Name	Имя инцидента.
DestinationUserName	Логин пользователя, которому назначили инцидент.
DestinationUserID	Идентификатор пользователя, которому назначили инцидент.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Алерт привязан к инциденту или алерт отвязан от инцидента или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	link alert to incident или unlink alert from incident
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который привязал алерт к инциденту или отвязал алерт от инцидента.
SourceUserID	Идентификатор пользователя, который привязал алерт к инциденту или отвязал алерт от инцидента.
ExternalID	Идентификатор инцидента.
Name	Имя инцидента.
DeviceFacility	Действие: привязать или отвязать.
DeviceCustomString1	Идентификатор алерта, который привязали или отвязали.
DeviceCustomString1Label	alert ID
DeviceCustomString2	Имя алерта, который привязали или отвязали.
DeviceCustomString2Label	alert name
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Зарегистрирован алерт Metrics для сервиса или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceCustomString6Label	tenant name
DeviceCustomString6	Название тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString2Label	Возможные значения: • QPS threshold reached • Failed Insert QPS threshold reached • High distribution queue • Low disk space • Low disk partition space • Output EventLoss increasing • Disk buffer size increasing • Enrichment errors increasing • High enrichment queue • Connector log errors increasing
DeviceCustomString2	created (время создания сервиса)
DeviceCustomString1Label	Порт API.
DeviceCustomNumber1	Продолжительность работы в секундах.
DeviceAction	service alert
EventOutcome	succeeded или failed

Событие привязано к алерту или отвязано от алерта или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	link event to alert или unlink event from alert
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который привязал или отвязал событие.
SourceUserID	Идентификатор пользователя, который привязал или отвязал событие.
ExternalID	Идентификатор алерта.
Name	Имя алерта.

DeviceFacility	Действие с событием: привязать или отвязать.
DeviceCustomString1	Идентификатор события, которое привязали или отвязали.
DeviceCustomString1Label	event ID
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Реагирование в Active Directory

Название поля события	Значение поля
DeviceAction	`ad response`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который применил реагирование.
SourceUserID	Идентификатор пользователя, который применил реагирование.
DeviceCustomString3	Наименование правила реагирования: CHANGE_PASSWORD, ADD_TO_GROUP, REMOVE_FROM_GROUP, BLOCK_USER.
DeviceCustomString3Label	`response rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DestinationUserName	Учетная запись пользователя Active Directory, на которую вызван ответ (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую вызван ответ.
DestinatinUserID	UUID учетной записи в KUMA.
FlexString1	Информация о группе, куда был добавлен или удален пользователь.
FlexString1Label	`group DN`

Создание поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	`extended field created`
EventOutcome	`succeeded`

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который создал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который создал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Редактирование поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field edited
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который редактировал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который редактировал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Импорт поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который импортировал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который импортировал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Импорт нормализатора с полем расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.

SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который импортировал нормализатор с полем расширенной схемы события.
SourceUserID	Идентификатор пользователя, который импортировал нормализатор с полем расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Удаление поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field deleted
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который удалил поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который удалил поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Отправлен запрос в KIRA

Название поля события	Значение поля
DeviceAction	KIRA task
EventOutcome	succeeded/ failed
SourceUserName	Логин пользователя, который использовался для отправки запроса.
SourceUserID	Идентификатор пользователя, который использовался для отправки запроса.
DeviceCustomString1	Итоговая отправленная строка.
DeviceCustomString1Label	cmd
DeviceCustomString2	Идентификатор события, из которого отправлен запрос.
DeviceCustomString2Label	event
DeviceCustomString3	Идентификатор задачи, созданной для отправки запроса.
DeviceCustomString3Label	task

Реагирование через KICS/KATA

Название поля события	Значение поля
DeviceAction	KICS response
DeviceAssetID	asset fqdn
DeviceFacility	manual response или automatic response

EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString3	Наименование правила ответа: Authorized, Not Authorized.
DeviceCustomString3Label	response rule name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DeviceExternalID	Идентификатор актива.
SourceHostName	FQDN актива.
Name	Название актива.
DeviceCustomString1	Перечень ip-адресов актива.
DeviceCustomString1Label	addresses
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString2	fdqn
DeviceCustomString2Label	fqdns

Реагирование через Kaspersky Automated Security Awareness Platform

Название поля события	Значение поля
DeviceAction	KASAP response
DeviceFacility	manual response
EventOutcome	succeeded или failed
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString1	Менеджер пользователя, на которого назначен курс.
DeviceCustomString1Label	manager
DeviceCustomString3	Информация о группе, где был пользователь. Отсутствует в случае failed.

DeviceCustomString3Label	manager
DeviceCustomString4	Информация о группе, куда добавили пользователя.
DeviceCustomString4Label	new kasap group
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DestinationUserID	Идентификатор учетной записи пользователя Active Directory, на которую происходит реагирование.
DestinationUserName	Имя учетной записи (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую происходит реагирование.

Реагирование через KEDR

Название поля события	Значение поля
DeviceAction	KEDR response
DeviceFacility	manual response или automatic response
EventOutcome	succeeded или failed
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
SourceAssetID	Идентификатор актива в KUMA, для которого производится реагирование. Значение не указывается, если реагирование производится по хешу или для всех активов.
DeviceExternalID	Параметр external ID, присвоенный KUMA в KEDR. Если external id один, при запуске по пользовательским хостам не заполняется.
DeviceCustomString1	Перечисление IP/FQDN-адресов актива для правила запрета для хоста по выбранному хешу из карточки события.
DeviceCustomString1Label	user defined list of ips or hostnames
DeviceCustomString2	Параметр sensor ID в KEDR (UUIDv4 | 'all' | 'custom').
DeviceCustomString2Label	sensor id of asset in KATA/EDR
ServiceID	Идентификатор сервиса, который вызвал реагирование. Заполняется только при автоматическом реагировании.
DeviceCustomString3	Наименование типа задачи: enable_network_isolation, disable_network_isolation, enable_prevention, disable_prevention, run_process.
DeviceCustomString3Label	kedr response kind
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Импорт техник и тактик MITRE ATT&CK

Название поля события	Значение поля
DeviceAction	import MITRE
EventOutcome	succeeded
FileID	Имя импортируемого файла.
SourceUserID	Идентификатор пользователя, который отправил запрос на импорт.
SourceUserName	Логин пользователя, который отправил запрос на импорт.

Резервное копирование Ядра KUMA и восстановление из резервной копии

Название поля события	Значение поля
DeviceAction	backup или restore
EventOutcome	succeeded или failed
SourceUserName	Логин пользователя, который выполнял резервное копирование или восстановление из резервной копии.
SourceUserID	Идентификатор пользователя, который выполнял резервное копирование или восстановление из резервной копии.
DeviceExternalID	Идентификатор сервиса Ядра KUMA.
Name	Имя сервиса Ядра KUMA.
FilePath	Полный путь хранения файла резервной копии.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта, которому принадлежит сервис Ядра KUMA.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Резервное копирование партиций, восстановление из резервной копии, импорт партиций из сторонней установки KUMA

Название поля события	Значение поля
DeviceAction	backup/restore/import
EventOutcome	succeeded или failed
SourceUserName	Логин пользователя, который выполнял резервное копирование партиций, восстановление из резервной копии или импорт партиций из сторонней установки KUMA.
SourceUserID	Идентификатор пользователя, который выполнял резервное копирование партиций, восстановление из резервной копии или импорт партиций из сторонней установки KUMA.

`DeviceExternalID`	Идентификатор сервиса хранилища.
`Name`	Имя хранилища.
`FilePath`	Полный путь хранения файла резервной копии. Полный путь, откуда должен быть выполнено восстановление из резервной копии или импорт партиций.
`Message`	Если `EventOutcome = failed`, в этом поле будет отображаться сообщение об ошибке.

Правила корреляции

В файле, доступном по ссылке для скачивания, описаны правила корреляции, включенные в поставку Kaspersky Unified Monitoring and Analysis Platform версии 4.2. Приводятся сценарии, покрываемые правилами, условия их использования и необходимые источники событий.

Одновременно возможно использование только одной из следующих версий набора SOC-правил:

- [OOTB] SOC Content - RU или [OOTB] SOC Content - ENG
- [OOTB] SOC Content - RU for KUMA 3.2 или [OOTB] SOC Content - ENG for KUMA 3.2
- [OOTB] KSC Package - RU или [OOTB] KSC Package - ENG
- [OOTB] KSMG Package - RU или [OOTB] KSMG Package - ENG
- [OOTB] KATA package - RU или [OOTB] KATA package - ENG
- [OOTB] Network Package - RU или [OOTB] Network Package - ENG
- [OOTB] PCIDSS Package - RU или [OOTB] PCIDSS Package - ENG
- [OOTB] XDR package - RU или [OOTB] XDR package - ENG
- [OOTB] UEBA package - RU или [OOTB] UEBA package - ENG
- [OOTB] PostgreSQL package - RU или [OOTB] PostgreSQL package - ENG

Правила корреляции можно импортировать в KUMA. См. раздел онлайн-справки *Импорт ресурсов*: https://support.kaspersky.com/KUMA/4.2/ru-RU/242787.htm.

Импортированные правила корреляции можно добавлять в используемые вашей организацией корреляторы. См. раздел онлайн-справки *Шаг 3. Корреляция*: https://support.kaspersky.com/KUMA/4.2/ru-RU/221168.htm.

Скачать описание правил корреляции KSC Package

Скачать описание правил корреляции KSMG Package

Скачать описание правил корреляции KATA Package

Скачать описание правил корреляции KUMA Package

Скачать описание правил корреляции Network Package

Скачать описание правил корреляции PCIDSS Package

Скачать описание правил корреляции SOC Content for KUMA

Скачать описание правил корреляции UEBA Package

Скачать описание правил корреляции XDR Package

Скачать описание правил корреляции PostgreSQL Package

Описание пакетов правил корреляции

В поставку Kaspersky Unified Monitoring and Analysis Platform версии 4.2 включены пакеты правил корреляции, перечисленные в таблице ниже.

Пакеты правил корреляции

Название пакета	Описание
[OOTB] SOC Content - RU	Пакет правил корреляции для KUMA версии 2.1 и выше с русской локализацией. Поддержка этого пакета прекращена.
[OOTB] SOC Content - ENG	Пакет правил корреляции для KUMA версии 2.1 и выше с английской локализацией. Поддержка этого пакета прекращена.
[OOTB] SOC Content - RU for KUMA 3.2	Пакет правил корреляции для KUMA версии 3.2 и выше с русской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] SOC Content - ENG for KUMA 3.2	Пакет правил корреляции для KUMA версии 3.2 и выше с английской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KUMA package - RU	Пакет правил корреляции для мониторинга событий KUMA. Правила корреляции позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. По событиям аудита решения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах решения, включая манипуляции с учетными записями и другими параметрами. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Также в пакет входят правила для мониторинга работоспособности служб. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] KUMA package - ENG	Пакет правил корреляции для мониторинга событий KUMA. Правила корреляции позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. По событиям аудита решения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах решения, включая манипуляции с учетными записями и другими параметрами. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Также в пакет входят правила для мониторинга работоспособности служб. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] KSC Package - RU	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Center. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. Он позволяет выявить потенциально опасные действия в системе на основе внутренних событий аудита. Для правильной работы правил корреляции необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Пакет правил корреляции работает на событиях, которые собираются через базу данных Kaspersky Security Center. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.

Название пакета	Описание
[OOTB] KSC Package - ENG	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Center. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. Он позволяет выявить потенциально опасные действия в системе на основе внутренних событий аудита. Для правильной работы правил корреляции необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Пакет правил корреляции работает на событиях, которые собираются через базу данных Kaspersky Security Center. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KSMG Package - RU	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Mail Gateway. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. Он позволяет выявить потенциально опасные действия в системе защиты почтового трафика на основе внутренних событий аудита. Для правильной работы правил необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Настройки аудита Kaspersky Secure Mail Gateway расположены в разделе **Параметры** → **Журналы и события** → **События**. В блоке **События аудита** нужно выбрать **Уровень журналирования событий аудита** → **Записывать события аудита и измененные параметры**. Примечания: • Пакет правил работает на событиях в формате CEF. • При отправке событий в SIEM-систему понадобится журнал Kaspersky Secure Mail Gateway в формате CEF (local2). Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KSMG Package - ENG	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Mail Gateway. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. Он позволяет выявить потенциально опасные действия в системе защиты почтового трафика на основе внутренних событий аудита. Для правильной работы правил необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Настройки аудита Kaspersky Secure Mail Gateway расположены в разделе **Параметры** → **Журналы и события** → **События**. В блоке **События аудита** нужно выбрать **Уровень журналирования событий аудита** → **Записывать события аудита и измененные параметры**. Примечания: • Пакет правил работает на событиях в формате CEF. • При отправке событий в SIEM-систему понадобится журнал Kaspersky Secure Mail Gateway в формате CEF (local2). Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KATA package - RU	Пакет правил корреляции для мониторинга событий Kaspersky Anti Targeted Attack (KATA) позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. По событиям аудита приложения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах приложения, включая манипуляции с учетными записями и отключение правил обнаружения. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] KATA package - ENG	Пакет правил корреляции для мониторинга событий Kaspersky Anti Targeted Attack (KATA) позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. По событиям аудита приложения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах приложения, включая манипуляции с учетными записями и отключение правил обнаружения. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] Network Package - RU	Пакет правил корреляции, направленных на выявление аномалий в сетевой активности, для KUMA версии 3.2 и выше с русской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK. Пакет также содержит панели мониторинга.
[OOTB] Network Package - ENG	Пакет правил корреляции, направленных на выявление аномалий в сетевой активности, для KUMA версии 3.2 и выше с английской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK. Пакет также содержит панели мониторинга.
[OOTB] PCIDSS Package - RU	Пакет правил корреляции, направленных на соблюдение требований стандарта PCI DSS. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. Этот пакет также содержит панели мониторинга. Для правильной работы набора ресурсов необходимо добавить поле расширенной схемы событий **S.Compliance_PCIDSS_Requirements** в разделе **Настройки** → **Другое** → **Поля расширенной схемы событий**. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.

Название пакета	Описание
[OOTB] PCIDSS Package - ENG	Пакет правил корреляции, направленных на соблюдение требований стандарта PCI DSS. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. Этот пакет также содержит панели мониторинга. Для правильной работы набора ресурсов необходимо добавить поле расширенной схемы событий **S.Compliance_PCIDSS_Requirements** в разделе **Настройки → Другое → Поля расширенной схемы событий**. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] XDR package - RU	Пакет содержит набор ресурсов для обнаружения продвинутых атак в инфраструктуре. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. С его помощью можно обнаружить не только попытки использования наиболее популярного, по версии Kaspersky MDR, вектора получения первоначального доступа - фишинга, но и вирусного заражения, попытки обхода средств защиты, доставки и запуска полезной нагрузки, закрепления, разведки, бокового перемещения и связи с сервером управления различными способами. Правила работают на событиях продуктов "Лаборатории Касперского": EDR, KSC, KSMG, а также используют события операционных систем семейства Windows. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] XDR package - ENG	Пакет содержит набор ресурсов для обнаружения продвинутых атак в инфраструктуре. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. С его помощью можно обнаружить не только попытки использования наиболее популярного, по версии Kaspersky MDR, вектора получения первоначального доступа - фишинга, но и вирусного заражения, попытки обхода средств защиты, доставки и запуска полезной нагрузки, закрепления, разведки, бокового перемещения и связи с сервером управления различными способами. Правила работают на событиях продуктов "Лаборатории Касперского": EDR, KSC, KSMG, а также используют события операционных систем семейства Windows. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] UEBA package - RU	Beta-версия пакета правил корреляции. Пакет правил корреляции предназначен для выявления аномального поведения учетной записи или рабочей станции в корпоративной сети. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. Он строит адаптивные модели нормального поведения на основе накопленных исторических данных (сбор данных длится месяц или заданный период). Эти модели используются для расчета статистических показателей, минимизирующих ложные срабатывания и эффективно выявляющих потенциально опасные отклонения. Источники данных: События ОС Windows, NetFlow, Cisco, Solar Proxy. Примечания: • Правила сбора данных (collection rules) могут быть адаптированы под конкретные средства защиты информации и источники телеметрии. • Для максимальной эффективности работы пакета критически важно обогащение событий данными DNS. • Правила могут оказать воздействие на производительность коррелятора. • Рекомендуется использовать правила в KUMA версии 4.0 и выше. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] UEBA package - ENG	Beta-версия пакета правил корреляции. Пакет правил корреляции предназначен для выявления аномального поведения учетной записи или рабочей станции в корпоративной сети. Пакет доступен для KUMA версии 3.2 и выше с английской локализацией. Он строит адаптивные модели нормального поведения на основе накопленных исторических данных (сбор данных длится месяц или заданный период). Эти модели используются для расчета статистических показателей, минимизирующих ложные срабатывания и эффективно выявляющих потенциально опасные отклонения. Источники данных: События ОС Windows, NetFlow, Cisco, Solar Proxy. Примечания: • Правила сбора данных (collection rules) могут быть адаптированы под конкретные средства защиты информации и источники телеметрии. • Для максимальной эффективности работы пакета критически важно обогащение событий данными DNS. • Правила могут оказать воздействие на производительность коррелятора. • Рекомендуется использовать правила в KUMA версии 4.0 и выше. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] NCCCI package - RU for KUMA 4.0	Пакет включает в себя набор панелей мониторинга и шаблонов отчетов, которые визуализируют детализированную информацию о нарушениях, классифицированных по категориям и типам инцидентов безопасности Национального координационного центра по компьютерным инцидентам (НКЦКИ). Визуализация строится на основе значений поля S.Compliance_NCCCI_IncidentClassification, которое автоматически заполняется правилом обогащения для правил из пакета SOC package. Перед импортом пакета визуализации необходимо создать строковое поле расширенной схемы событий S.Compliance_NCCCI_IncidentClassification, либо убедиться в его наличии. Данный пакет также содержит панели мониторинга.

Название пакета	Описание
[OOTB] FSTEC package - RU for KUMA 4.0	Пакет включает в себя набор панелей мониторинга и шаблонов отчетов, которые визуализируют детализированную информацию о нарушениях защитных мер, рекомендуемых ФСТЭК России для предотвращения угроз и устранения уязвимостей согласно информации Банка данных угроз безопасности информации. Визуализация строится на основе значений поля S.Compliance_FSTEC_ProtectiveMeasures, которое автоматически заполняется правилом обогащения для правил из пакета SOC package. Перед импортом пакета визуализации необходимо создать строковое поле расширенной схемы событий S.Compliance_FSTEC_ProtectiveMeasures, либо убедиться в его наличии. Данный пакет также содержит панели мониторинга.
[OOTB] PostgreSQL package - RU [OOTB] PostgreSQL package - ENG	Пакет правил корреляции для мониторинга событий PostgreSQL. Правила корреляции позволяют выявлять потенциально опасные действия в системе на основе внутренних событий аудита. По событиям аудита приложения обнаруживаются аномалии в поведении пользователей, такие как сбор информации об учетных записях, попытки выполнения произвольного кода в системе, а также запись и чтение данных из файловой системы. Для корректной работы правил корреляции необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации.

Автоматическое подавление срабатывания правил

В пакете с правилами корреляции SOC_package предусмотрено автоматическое подавление срабатывания правил, если частота срабатывания превышает пороговые значения.

Опция автоматического подавления предполагает следующую логику работы: если правило сработало более 100 раз за 1 минуту и такое поведение случилось не менее 5 раз за 10 минут, правило будет помещено в стоп-лист.

- При первом помещении в стоп-лист правило отключается на 1 час.
- При повторном - на 24 часа.
- При всех последующих на 7 дней.

Логика работы описана в ресурсах: правилах, активных листах и словарях, которые размещены в папке SOC_package/System/Rule disabling by condition.

Вы можете задать параметры и пороговые значения с учетом своих потребностей.

Чтобы включить опцию автоматического подавления, в словаре SOC_package/Integration/Rule disabling configuration присвойте параметру **enable** значение `1`.

Чтобы отключить опцию автоматического подавления, в словаре SOC_package/Integration/Rule disabling configuration присвойте параметру **enable** значение `0`.

По умолчанию автоматическое подавление включено и параметру **enable** присвоено значение `1`.

События аудита

В правилах корреляции из набора ресурсов [OOTB] SOC Content используются события аудита, перечисленные в таблице ниже.

Источник событий	События аудита
CheckPoint	Anti Malware, Threat Emulation
Cisco ASA, FTD, PIX	106021, 320001, 322001, 322002, 322003, 405001, 405002
CyberTrace	alert
DNS	query
KATA	TAA has tripped on events database
KSC	GNRL_EV_ATTACK_DETECTED, GNRL_EV_SUSPICIOUS_OBJECT_FOUND, GNRL_EV_VIRUS_FOUND, GNRL_EV_WEB_URL_BLOCKED, KLSRV_HOST_STATUS_CRITICAL, KLSRV_HOST_STATUS_OK, KLSRV_HOST_STATUS_WARNING
KSMG	LMS_EV_SCAN_LOGIC_AV_STATUS, LMS_EV_SCAN_LOGIC_KT_STATUS, LMS_EV_SCAN_LOGIC_CF_STATUS, LMS_EV_SCAN_LOGIC_AP_STATUS
KUMA	Correlation rule
Windows Event Log Powershell	4103, 4104
Windows Event Log Security	1102, 4624, 4625, 4656, 4657, 4662, 4663, 4672, 4688, 4697, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4768, 4769, 4771, 5136, 5140, 5145
Windows Event Log System	7036, 7045
Windows Event Log Defender	1006, 1015, 1116, 1117, 5001, 5010, 5012, 5101
Netflow, FW	Traffic log
Palo Alto	virus
auditd	ADD_USER, DEL_USER, PATH, SYSCALL, USER_AUTH, USER_LOGIN, execve

[▷]

https://rutube.ru/video/a37c939ed992377b38a592503ef4d983/

https://rutube.ru/video/cc57b965e06574165617b37ea1d8ac96/

Отправка тестовых событий в KUMA

В KUMA предусмотрена отправка тестовых событий в систему. Используйте опцию отправки тестовых событий в KUMA, чтобы проверить работу правил, отчетов, панелей мониторинга, а также чтобы проверить потребление ресурсов коллектором при разных потоках событий. События можно отправить только в коллектор, осуществляющий прием по протоколу TCP или http.

Для отправки тестовых событий вам понадобится:

- Файл kuma, запущенный с определенными параметрами.

  В инструкции ниже файл с сырыми событиями назван send_test_events.txt в качестве примера. Вы можете использовать собственное название файла.

- Конфигурационный файл, в котором вы определите параметры запуска исполняемого файла.

  В инструкции ниже конфигурационный файл назван config_for_test_events в качестве примера. Вы можете использовать собственное название файла.

Чтобы отправить тестовые события:

1. Получите примеры событий, которые необходимо отправить в KUMA:

   a. В веб-интерфейсе KUMA в разделе **События** в правом верхнем углу нажмите значок ⚙ и появившемся окне на вкладке **Столбцы полей событий** установите флажок для поля **Raw**. В окне **События** появится столбец Raw.

   b. Выполните поиск событий.

   c. Экспортируйте результаты поиска: в окне **События** в правом верхнем углу нажмите ... и выберите **Экспортировать в формат TSV**.

   d. Перейдите в раздел KUMA **Диспетчер задач** и нажмите на задачу **Экспорт событий**, в появившемся контекстном меню выберите **Скачать**.

   В разделе Загрузки появится файл `<имя файла с экспортированными событиями>`.tsv

   Если сбор сырых событий не выполняется, включите сбор на короткое время, выбрав в параметре нормализатора **Сохранить исходное событие** значение **Всегда**. После выполнения сбора, верните параметру **Сохранить исходное событие** прежнее значение.

e. Создайте текстовый файл send_test_events.txt и скопируйте содержимое поля `Raw` из `<имя файла с экспортированными событиями>`.tsv в текстовый файл send_test_events.txt.

f. Сохраните send_test_events.txt.

2. Создайте конфигурационный файл config_for_test_events и добавьте в файл следующие строки:

```
{
"kind": "<tcp или http>",
"name": "-",
"connection": {
"name": "-",
"kind": "<tcp или http>",
"urls": ["< IP коллектора KUMA для приема событий по протоколу TCP >:< порт коллектора KUMA для приема событий по протоколу TCP >"]
}
}
```

Сохраните конфигурационный файл config_for_test_events.

3. Убедитесь, что между сервером, выполняющим отправку событий и сервером, на котором установлен коллектор, обеспечена сетевая связанность.

4. Чтобы отправить содержимое файла с тестовыми событиями в коллектор KUMA, выполните следующую команду:

```
/opt/kaspersky/kuma/kuma tools load --raw --events /home/events/send_test_events.txt --cfg home/events/config_for_test_events --limit 1500 --replay 100000
```

Доступные параметры

Параметр	Описание
`--events`	Полный путь к файлу, содержащему сырые события. Обязательный параметр. Если полный путь не указан, команда не будет выполнена.
`--cfg`	Путь к конфигурационному файлу. Обязательный параметр. Если полный путь не указан, команда не будет выполнена.
`--limit`	Поток событий в секунду (EPS), который будет направлен в коллектор. Обязательный параметр. Если значение не указано, команда не будет выполнена.
`--replay`	Количество событий, которое требуется отправить. Обязательный параметр. Если значение не указано, команда не будет выполнена. Шаг --replay составляет 10000. Минимальное значение: 10000. При --replay 16 отправится 10000 событий. При --replay 16000 отправится 20000 событий.

В результате выполнения команды тестовые события успешно отправлены в коллектор KUMA. Вы можете проверить поступление тестовых событий, выполнив поиск связанных событий в веб-интерфейсе KUMA.

Формат времени

KUMA поддерживает обработку информации, передающейся в поля Модели данных события с типом timestamp (EndTime, StartTime, DeviceCustomDate1, и т.д.) в следующих форматах:

- "May 8, 2009 5:57:51 PM".
- "oct 7, 1970".
- "oct 7, '70".
- "oct. 7, 1970".
- "oct. 7, 70".
- "Mon Jan 2 15:04:05 2006".
- "Mon Jan 2 15:04:05 MST 2006".
- "Mon Jan 02 15:04:05 -0700 2006".
- "Monday, 02-Jan-06 15:04:05 MST".
- "Mon, 02 Jan 2006 15:04:05 MST".
- "Tue, 11 Jul 2017 16:28:13 +0200 (CEST)".
- "Mon, 02 Jan 2006 15:04:05 -0700".
- "Mon 30 Sep 2018 09:09:09 PM UTC".
- "Mon Aug 10 15:44:11 UTC+0100 2015".
- "Thu, 4 Jan 2018 17:53:36 +0000".
- "Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)".
- "Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)".
- "September 17, 2012 10:09am".
- "September 17, 2012 at 10:09am PST-08".
- "September 17, 2012, 10:10:09".
- "October 7, 1970".
- "October 7th, 1970".
- "12 Feb 2006, 19:17".
- "12 Feb 2006 19:17".

- "14 May 2019 19:11:40.164".
- "7 oct 70".
- "7 oct 1970".
- "03 February 2013".
- "1 July 2013".
- "2013-Feb-03".

Формат dd/Mon/yyyy

- "06/Jan/2008:15:04:05 -0700".
- "06/Jan/2008 15:04:05 -0700".

Формат mm/dd/yyyy

- "3/31/2014".
- "03/31/2014".
- "08/21/71".
- "8/1/71".
- "4/8/2014 22:05".
- "04/08/2014 22:05".
- "4/8/14 22:05".
- "04/2/2014 03:00:51".
- "8/8/1965 12:00:00 AM".
- "8/8/1965 01:00:01 PM".
- "8/8/1965 01:00 PM".
- "8/8/1965 1:00 PM".
- "8/8/1965 12:00 AM".
- "4/02/2014 03:00:51".

- "03/19/2012 10:11:59".
- "03/19/2012 10:11:59.3186369".

Формат yyyy/mm/dd

- "2014/3/31".
- "2014/03/31".
- "2014/4/8 22:05".
- "2014/04/08 22:05".
- "2014/04/2 03:00:51".
- "2014/4/02 03:00:51".
- "2012/03/19 10:11:59".
- "2012/03/19 10:11:59.3186369".

Формат yyyy:mm:dd

- "2014:3:31".
- "2014:03:31".
- "2014:4:8 22:05".
- "2014:04:08 22:05".
- "2014:04:2 03:00:51".
- "2014:4:02 03:00:51".
- "2012:03:19 10:11:59".
- "2012:03:19 10:11:59.3186369".

Формат, содержащий китайские символы

"2014年04月08日"

Формат yyyy-mm-ddThh

- "2006-01-02T15:04:05+0000".
- "2009-08-12T22:15:09-07:00".
- "2009-08-12T22:15:09".
- "2009-08-12T22:15:09.988".
- "2009-08-12T22:15:09Z".
- "2017-07-19T03:21:51:897+0100".
- "2019-05-29T08:41-04" без указания секунд, 2 символа TZ.

Формат yyyy-mm-dd hh:mm:ss

- "2014-04-26 17:24:37.3186369".
- "2012-08-03 18:31:59.257000000".
- "2014-04-26 17:24:37.123".
- "2013-04-01 22:43".
- "2013-04-01 22:43:22".
- "2014-12-16 06:20:00 UTC".
- "2014-12-16 06:20:00 GMT".
- "2014-04-26 05:24:37 PM".
- "2014-04-26 13:13:43 +0800".
- "2014-04-26 13:13:43 +0800 +08".
- "2014-04-26 13:13:44 +09:00".
- "2012-08-03 18:31:59.257000000 +0000 UTC".
- "2015-09-30 18:48:56.35272715 +0000 UTC".
- "2015-02-18 00:12:00 +0000 GMT".
- "2015-02-18 00:12:00 +0000 UTC".
- "2015-02-08 03:02:00 +0300 MSK m=+0.000000001".

- "2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001".
- "2017-07-19 03:21:51+00:00".
- "2014-04-26".
- "2014-04".
- "2014".
- "2014-05-11 08:20:13,787".

Формат yyyy-mm-dd-07:00

"2020-07-20+08:00"

Формат mm.dd.yyyy

- "3.31.2014".
- "03.31.2014".
- "08.21.71".

Формат yyyy.mm.dd

- "2014.03.30"

Формат yyyymmdd и аналогичные

- "20140601".
- "20140722105203".

Формат yymmdd hh:mm:yy

"171113 14:14:20"

Формат Unix timestamp

- "1332151919".
- "1384216367189".
- "1384216367111222".
- "1384216367111222333".

Сопоставление полей предустановленных нормализаторов

В файле, доступном по ссылке для скачивания, представлено описание сопоставления полей предустановленных нормализаторов.

Скачать Описание сопоставления полей предустановленных нормализаторов

Устаревшие ресурсы

Список устаревших ресурсов

Название	Тип ресурса	Описание
[Deprecated][OOTB] Microsoft SQL Server xml	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.2. Если вы использовали этот нормализатор, необходимо перейти к использованию нормализатора [OOTB] Microsoft Products for KUMA 3.
[Deprecated][OOTB] Windows Basic	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.2. Если вы использовали этот нормализатор, необходимо перейти к использованию нормализатора [OOTB] Microsoft Products for KUMA 3.
[Deprecated][OOTB] Windows Extended v.0.3	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.2. Если вы использовали этот нормализатор, необходимо перейти к использованию нормализатора [OOTB] Microsoft Products for KUMA 3.
[Deprecated][OOTB] Cisco ASA Extended v 0.1	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.2. Если вы использовали этот нормализатор, необходимо перейти к использованию нормализатора [OOTB] Cisco ASA and IOS syslog.
[Deprecated][OOTB] Cisco Basic	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.2. Если вы использовали этот нормализатор, необходимо перейти к использованию нормализатора [OOTB] Cisco ASA and IOS syslog.
[Deprecated][OOTB] Linux audit and iptables syslog	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.4. В KUMA 3.2 мы рекомендуем использовать нормализатор [OOTB] Linux auditd syslog for KUMA 3.2.
[Deprecated][OOTB] Linux audit.log file	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.4. В KUMA 3.2 мы рекомендуем использовать нормализатор [OOTB] Linux auditd file for KUMA 3.2.
[OOTB] Checkpoint Syslog CEF by CheckPoint	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.4. В KUMA 3.4 и более новых версиях системы мы рекомендуем использовать нормализатор [OOTB] Checkpoint syslog.

Название	Тип ресурса	Описание
[OOTB] Eltex MES Switches	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.4. В KUMA 3.4 и более новых версиях системы мы рекомендуем использовать нормализаторы [OOTB] Eltex MES syslog, [OOTB] Eltex ESR syslog.
[OOTB] PTsecurity NAD	Нормализатор	Нормализатор удален из набора ресурсов в KUMA 3.4. В KUMA 3.4 и более новых версиях системы мы рекомендуем использовать нормализатор [OOTB] PTsecurity NAD json
[OOTB][AD] Granted TGS without TGT (Golden Ticket)	Правило	Правило было удалено из набора ресурсов KUMA 3.4.
[OOTB][AD] Possible Kerberoasting attack	Правило	Правило было удалено из набора ресурсов KUMA 3.4.
[OOTB][AD][Technical] 4768. TGT Requested	Правило	Правило было удалено из набора ресурсов KUMA 3.4.
[OOTB][AD] List of requested TGT. EventID 4768	Активный лист	Список был удален из набора ресурсов KUMA 3.4.
[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	Нормализатор	Нормализатор устарел и был удален из набора ресурсов KUMA 4.6. Мы рекомендуем использовать нормализатор [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog.
[OOTB] VipNet Coordinator Syslog Direction	Словарь	Словарь [OOTB] VipNet Coordinator Syslog Direction устарел и был удален из набора ресурсов KUMA 4.6.

Генерация событий для тестирования работы нормализатора

При необходимости вы можете самостоятельно сгенерировать примеры событий, чтобы проверить работу написанного нормализатора. Такая проверка упрощает написание регулярных выражений и позволяет увидеть, какие значения попадают в поля событий KUMA.

Стоит принять во внимание следующие особенности:

- Эта проверка эмулирует обработку события. Указанные примеры события в поле **Пример события** предназначены для отображения примеров в разделе **Сопоставление полей**. Из примеров родительского нормализатора формируются примеры дочерних нормализаторов с учетом параметра **Поле, которое следует передать в нормализатор**.

- Невозможно применять мутации.

Чтобы протестировать нормализатор, необходимо добавить пример события в поле **Пример события** в выбранном нормализаторе и запустить генерацию событий с помощью соответствующей команды. В результате выполнения команды KUMA берет пример события из поля **Пример события** и посылает события в нормализатор с указанным интервалом. При необходимости вы можете указать несколько примеров, чтобы получить события для нескольких примеров.

Чтобы протестировать нормализатор:

1. Выберите коллектор, на котором вы планируете проводить тестирование:

   - Если коллектор установлен на сервере и запущен, остановите сервис коллектора:

     ```
     sudo systemctl stop kuma-collector-<идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA>.service
     ```

   - Если коллектор не запущен или в процессе создания или редактирования, перейдите к следующему шагу.

2. В мастере создания коллектора при необходимости заполните или отредактируйте обязательные поля на шаге **Подключение источников** и на шаге **Транспорт**, а затем перейдите к шагу **Парсинг**:

   a. Привяжите нормализатор, выбрав его из раскрывающегося списка, или создайте нормализатор.

   b. В поле **Примеры событий** добавьте примеры событий. Например, для нормализатора типа json вы можете добавить следующее значение: `{"name": "test_events", "address": "10.12.12.31"}`. Вы можете указать несколько примеров, чтобы в одном нормализаторе получать события по нескольким примерам. События будут генерироваться для каждого примера.

3. В мастере установки коллектора перейдите к шагу **Маршрутизация** и укажите хранилище, где будут храниться тестовые события.

4. Проверьте параметры коллектора и нажмите **Сохранить**.

5. Перейдите в раздел KUMA **Активные сервисы** и добавьте коллектор с помощью кнопки **Добавить**. В открывшемся окне **Выберите сервис** выберите коллектор и нажмите **Создать сервис**. Коллектор отобразится в списке **Активные сервисы**.

6. Проверьте статус коллектора, на который поступают события. Статус коллектора должен быть красным.

7. Выполните команду генерации событий с необходимыми параметрами:

   - Если коллектор не установлен на сервер, а только добавлен в разделе **Активные сервисы**:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core <FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --generator.interval <значение интервала генерации и отправки событий в секундах> --id <идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA> --api.port <номер свободного, неиспользуемого порта API>
     ```

     Если значение интервала генерации и отправки событий не указано или равно нулю, события не будут генерироваться.

   - Если коллектор установлен на сервере:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --generator.interval <значение интервала генерации и отправки событий в секундах> --id <идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA> --api.port <номер свободного, неиспользуемого порта API>
     ```

     Если значение интервала генерации и отправки событий не указано или равно нулю, события не будут генерироваться.

В результате KUMA сгенерирует события и отправит их в нормализатор с учетом указанного интервала.

Вы можете проверить, что события созданы и соответствуют ожиданиям, в разделе **События**. Дополнительную информацию о проверке вы можете посмотреть в файле /etc/systemd/system/multi-user.target.wants/kuma-collector-<идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA>.service.

Если полученный результат не соответствует ожиданиям, измените пример события:

- Если коллектор не установлен на сервер и добавлен только в разделе **Активные сервисы**, внесите изменения в поле **Пример события** в нормализаторе коллектора и сохраните параметры коллектора.
- Если коллектор установлен на сервер и остановлен как сервис, внесите изменения в поле **Пример события** в нормализаторе коллектора, сохраните параметры коллектора, перейдите в раздел **Активные сервисы**, выберите коллектор и обновите параметры коллектора, нажав на кнопку **Обновить**.

Если полученный результат соответствует ожиданиям:

1. Отключите генерацию событий, например, нажав **Ctrl+C** в консоли интерпретатора командной строки.
2. Запустите сервис коллектора, если сервис уже установлен на сервер, но был ранее остановлен:

   ```
   sudo systemctl start kuma-collector-<идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA>.service
   ```

3. Если коллектор только добавлен в раздел **Активные сервисы**, но еще не установлен на сервер, установите коллектор на сервер с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core <FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса коллектора, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install
   ```

Глоссарий

SELinux (Security-Enhanced Linux)

Система контроля доступа процессов к ресурсам операционной системы на основе использования политик безопасности.

SIEM

Security Information and Event Management system – система управления информацией о безопасности и событиями безопасности. Решение для управления информацией и событиями в системе безопасности компании.

STARTTLS

Расширение обычного протокола текстового обмена, которое позволяет создать зашифрованное соединение (TLS или SSL) прямо поверх обычного TCP-соединения вместо открытия для шифрованного соединения отдельного порта.

UserPrincipalName

UserPrincipalName (UPN) – это имя пользователя в формате адреса электронной почты, например `username@domain.com`.

UPN-имя необязательно должно соответствовать фактическому адресу электронной почты пользователя. В этом примере `username` – это имя пользователя в домене Active Directory (user logon name), а `domain.com` – это UPN-суффикс. Между ними используется разделитель `@`. По умолчанию в Active Directory в качестве UPN-суффикса используется DNS-имя домена Active Directory.

Агрегация

Объединение нескольких однотипных сообщений из источника события в одно событие.

Веб-интерфейс KUMA

Служба KUMA, которая предоставляет пользовательский интерфейс для настройки и отслеживания операций KUMA.

Кластер

Группа серверов, на которых установлено решение KUMA и которые были сгруппированы для централизованного управления с помощью веб-интерфейса решения.

Коллектор

Компонент KUMA, который получает сообщения из источников событий, обрабатывает их и передает в хранилище, коррелятор и/или сторонние сервисы для выявления подозрений на инциденты ИБ (алерты).

Коннектор

Компонент KUMA, обеспечивающий транспорт для приема данных из внешних систем.

Корреляционное правило

Ресурс KUMA, используемый для распознавания заданных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания.

Нормализатор

Компонент системы, отвечающий за процесс обработки сырых событий, поступающих от источников событий. Один нормализатор обрабатывает события от одного устройства или программного обеспечения одной конкретной версии.

Нормализация

Процесс приведения данных, составляющих событие, в соответствие с полями модели данных события KUMA. Во время нормализации могут выполняться определенные преобразования данных по заданным правилам, например, символы верхнего регистра могут заменяться на символы нижнего регистра, определенные последовательности символов могут перезаписываться другими и т.п.

Обогащение

Преобразование текстовых данных события с использованием словарей, констант, вызовов службы DNS и других инструментов.

Отчет

Ресурс KUMA, который используется, чтобы сформировать набор данных по критериям фильтра, заданным пользователем.

Панель мониторинга

Компонент системы KUMA, выполняющий визуализацию данных.

Парсинг

Процесс организации данных и приведения поступающих событий в формат KUMA.

Роль

Набор прав доступа, установленных для предоставления пользователю веб-интерфейса KUMA полномочий для выполнения задач.

Сетевой порт

Параметр протокола TCP и UDP, который определяет место назначения пакетов данных в формате IP, которые передаются на узел по сети, и позволяет различным программам, работающим на одном узле, получать данные независимо друг от друга. Каждая программа обрабатывает данные, отправленные на определенный порт (иногда говорят, что программа прослушивает этот номер порта).

Стандартной практикой является присвоение стандартных номеров портов определенным распространенным сетевым протоколам (например, веб-серверы обычно получают данные через HTTP на TCP-порт 80), хотя в целом программа может использовать любой протокол на любом порту. Возможные значения: от 1 до 65 535.

Событие

Случай активности сетевых устройств, прикладного программного обеспечения, средств защиты информации, операционных систем и иных устройств, который можно обнаружить и записать. Например, к событиям относятся: событие успешного входа пользователя, событие очистки журнала, событие отключения антивирусного ПО.

Сырое событие

Событие, не прошедшее этап нормализации в KUMA.

Фильтр

Набор условий, которые решение использует для выбора событий для дальнейшей обработки.

Информация о стороннем коде

Информация о стороннем коде содержится в файле LEGAL_NOTICES, расположенном в директории /opt/kaspersky/kuma/LEGAL_NOTICES.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

AMD – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Apache, Apache Cassandra, Apache Tomcat являются либо зарегистрированными товарными знаками, либо товарными знаками Apache Software Foundation в Соединенных Штатах и/или других странах.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

Cisco, IOS, Snort являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, Citrix NetScaler являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Dameware, SolarWinds – товарные знаки, права на которые принадлежат компании SolarWinds Worldwide, LLC или аффилированным лицам компании, зарегистрированы в Бюро по патентам и товарным знакам США, а также могут быть зарегистрированы или находиться в процессе регистрации в других странах.

Dell Technologies, Dell и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

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.

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, FortiOS, FortiSOAR – товарные знаки или зарегистрированные в США и/или других странах товарные знаки Fortinet, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Chrome, Google Chrome – товарные знаки Google LLC.

HUAWEI, Huawei Eudemon являются товарными знаками Huawei Technologies Co., Ltd.

IBM, Guardium, InfoSphere – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Core являются товарными знаками Intel Corporation или ее дочерних компаний.

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.

Mac – товарный знак Apple Inc.

Microsoft, Active Directory, AppLocker, Azure, Excel, Halo, Hyper-V, Lync, Office 365, Outlook, PowerShell, SharePoint, Skype, SQL Server, Windows, Windows PowerShell и Windows Server являются товарными знаками группы компаний Microsoft.

Mozilla и 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.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

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.

Название CommuniGate Pro – товарный знак или зарегистрированный товарный знак Stalker Software, Inc.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

OpenAPI – товарный знак компании The Linux Foundation.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Rocky Linux является товарным знаком The Rocky Enterprise Software 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.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

ClickHouse является зарегистрированным товарным знаком ClickHouse, Inc. https://clickhouse.com/

Zabbix – зарегистрированный товарный знак Zabbix SIA.

ViPNet является зарегистрированным товарным знаком компании "ИнфоТеКС".

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.

Известные ограничения и проблемы

KUMA имеет ряд ограничений, не критичных для работы решения:

- После обновления KUMA 3.4 до версии 4.0.1 в разделе **Параметры** → **Другое** → **Мониторинг сервисов** значение параметра **Detached parts threshold, % (Порог места на диске, занимаемого отделенными частями, %)** сбрасывается до 0.

- После обновления KUMA 3.4 до версии 4.0 некоторые виджеты на панели мониторинга отображаются с ошибкой. Для исправления ошибки обновите данные на панели мониторинга вручную или дождитесь автоматического обновления.

- Форма виджета может открыться под формой настроек **Панели мониторинга**, если перейти по ссылкам из колонки **Использовано в виджетах**, в случае, когда до открытия формы настроек **Панели мониторинга** уже открывались настройки какого-либо виджета.