kaspersky

Kaspersky LogAnalyzer

© 2025 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky LogAnalyzer

О программе LogAnalyzer

- Комплект поставки
- Аппаратные и программные требования
- Интерфейс LogAnalyzer
- Совместимость с другими программами

Архитектура программы

- Ядро
- Коллектор
- Хранилище
- Основные сущности
  - О тенантах
  - О событиях
  - Об активах
  - О ресурсах
  - О сервисах
  - Об агентах

Лицензирование программы

- О Лицензионном соглашении
- О лицензии
- О Лицензионном сертификате
- О лицензионном ключе
- О файле ключа
- О лицензионном коде
- Предоставление данных в Kaspersky LogAnalyzer
- Добавление лицензионного ключа в веб-интерфейс программы
- Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы
- Удаление лицензионного ключа в веб-интерфейсе программы

Руководство администратора

- Установка и удаление LogAnalyzer
  - Требования к установке программы
    - Обновление с операционной системы Oracle Linux 8.x до Oracle Linux 9.x
  - Порты, используемые LogAnalyzer при установке
  - Скачивание CA-сертификатов
  - Перевыпуск внутренних CA-сертификатов
  - Изменение самоподписанного сертификата веб-консоли
  - Синхронизация времени на серверах
  - О файле инвентаря
    - Параметры конфигурации LogAnalyzer в файле инвентаря
  - Установка на одном сервере
    - Подготовка файла инвентаря single.inventory.yml
    - Установка программы на одном сервере
  - Распределенная установка

- Подготовка контрольной машины
- Подготовка целевой машины
- Подготовка файла инвентаря distributed.inventory.yml
- Установка программы в распределенной конфигурации
- Распределенная установка с Ядром LogAnalyzer в кластере Kubernetes
- Дополнительные требования при развертывании Ядра в Kubernetes
- Установка LogAnalyzer в кластере Kubernetes
- Подготовка контрольной машины
- Подготовка целевой машины
- Подготовка файла инвентаря k0s.inventory.yml
- Установка программы в отказоустойчивой конфигурации
- Перенос Ядра LogAnalyzer в новый кластер Kubernetes
- Доступность Ядра LogAnalyzer при различных сценариях
- Управление Kubernetes и доступ к LogAnalyzer
- Часовой пояс в кластере Kubernetes
- Распределенная установка с Ядром LogAnalyzer в кластере Raft
- Подготовка контрольной машины
- Подготовка целевой машины
- Подготовка файла инвентаря distributed.inventory.yml для установки LogAnalyzer с несколькими сервисами Ядра LogAnalyzer в кластере Raft
- Установка LogAnalyzer в кластере Raft
- Расширение кластера Raft
- Поддерживаемые сценарии установки и обновления с 3.4.x до 4.x с установкой Ядра в кластере Raft
- Резервное копирование LogAnalyzer
- Изменение конфигурации LogAnalyzer
- Обновление предыдущих версий LogAnalyzer
- Устранение ошибок при обновлении
- Удаление LogAnalyzer

Работа с тенантами
- Выбор тенанта
- Правила принадлежности к тенантам

Управление пользователями
- Роли пользователей
- Настройка политики безопасности при входе в веб-интерфейс LogAnalyzer
- Создание пользователя
- Изменение учетной записи пользователя
- Особенности изменения набора пространств, назначенных пользователю

Сервисы LogAnalyzer
- Инструменты сервисов
- Получение идентификатора сервиса
- Остановка, запуск и проверка статуса сервиса
- Перезапуск сервиса
- Удаление сервиса
- Окно Разделы
- Поиск связанных событий
- Наборы ресурсов для сервисов
- Создание хранилища

- Структура кластера ClickHouse
- Параметры узлов кластера ClickHouse
- Холодное хранение событий
  - Удаление дисков холодного хранения
  - Отключение, архивирование и подключение партиций
- Создание набора ресурсов для хранилища
- Создание сервиса хранилища в веб-интерфейсе LogAnalyzer
- Установка хранилища в сетевой инфраструктуре LogAnalyzer
- 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 LogAnalyzer
  - 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 LogAnalyzer
  - Автоматически созданные агенты
  - Установка агента в сетевой инфраструктуре LogAnalyzer
    - Установка агента LogAnalyzer на устройствах Linux
    - Установка агента LogAnalyzer на устройствах Windows
  - Обновление агентов
  - Передача в LogAnalyzer 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 LogAnalyzer событий с машин Windows
  - Импорт файла со списком серверов для агентов WMI
- Настройка источников событий

Настройка получения событий Auditd
Настройка коллектора LogAnalyzer для получения событий Auditd
Настройка сервера источника событий с помощью сервиса rsyslog
Настройка получения событий KATA/EDR
Настройка передачи событий KATA/EDR в LogAnalyzer
Создание коллектора LogAnalyzer для получения событий KATA/EDR
Установка коллектора LogAnalyzer для получения событий KATA/EDR
Настройка передачи событий Kaspersky Security Center в SIEM-систему LogAnalyzer
Настройка передачи событий Kaspersky Security Center в формате CEF
Настройка коллектора LogAnalyzer для сбора событий Kaspersky Security Center
Установка коллектора LogAnalyzer 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 LogAnalyzer
Настройка коннектора
Настройка коллектора LogAnalyzer для получения событий Kaspersky Security Center из MS SQL
Установка коллектора LogAnalyzer для получения событий Kaspersky Security Center из MS SQL
Настройка получения событий с устройств Windows с помощью Агента LogAnalyzer (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 LogAnalyzer для получения событий с устройств Windows
Установка коллектора LogAnalyzer для получения событий с устройств Windows
Настройка передачи в LogAnalyzer событий с устройств Windows с помощью Агента LogAnalyzer (WEC)
Настройка получения событий с устройств Windows с помощью Агента LogAnalyzer (WMI)
Настройка параметров аудита для работы с LogAnalyzer
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 LogAnalyzer
Настройка получения событий КриптоПро NGate
Настройка передачи событий КриптоПро NGate в LogAnalyzer

Настройка получения событий Ideco UTM
Настройка передачи событий Ideco UTM в LogAnalyzer
Настройка получения событий KWTS
Настройка передачи событий KWTS в LogAnalyzer
Настройка получения событий KLMS
Настройка передачи событий KLMS в LogAnalyzer
Настройка получения событий KSMG
Настройка передачи событий KSMG в LogAnalyzer
Настройка получения событий KICS for Networks
Создание коннектора KICS for Networks для передачи событий в LogAnalyzer
Настройка передачи событий KICS for Networks в LogAnalyzer
Создание коллектора LogAnalyzer для получения событий KICS for Networks
Настройка получения событий PT NAD
Настройка передачи событий PT NAD в LogAnalyzer
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 LogAnalyzer
Настройка получения событий FreeIPA
Настройка передачи событий FreeIPA в LogAnalyzer
Настройка получения событий VipNet TIAS
Настройка передачи событий VipNet TIAS в LogAnalyzer
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 LogAnalyzer для получения и обработки событий Postfix

- Настройка получения событий CommuniGate Pro
  - Настройка CommuniGate Pro для отправки событий
  - Настройка коллектора LogAnalyzer 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

Мониторинг источников событий

- Состояние источников
  - Список источников событий
- Политики мониторинга

Интеграция с другими решениями

- 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
- Аутентификация с помощью доменных учетных записей
  - Включение и выключение доменной аутентификации
  - Настройка соединения KUMA с FreeIPA
  - Настройка соединения LogAnalyzer с Active Directory
  - Настройка соединения LogAnalyzer с Active Directory Federation Services
    - Настройка подключения на стороне Active Directory Federation Services
    - Устранение ошибки Access denied
- Интеграция с NeuroDAT SIEM IM
- Импорт информации об активах из RedCheck
- Настройка получения событий Sendmail
  - Настройка журналирования Sendmail
  - Настройка передачи событий Sendmail

Управление LogAnalyzer

- Вход в веб-интерфейс приложения
- Мониторинг сервисов
  - Просмотр метрик LogAnalyzer
- Работа с задачами LogAnalyzer

- Просмотр таблицы задач
- Настройка отображения таблицы задач
- Просмотр результата выполнения задачи
- Повторный запуск задачи
- Подключение к SMTP-серверу
- Уведомления LogAnalyzer
- Журналы LogAnalyzer
- Работа с геоданными
- Формат геоданных
- Конвертация геоданных из MaxMind и IP2Location
- Импорт и экспорт геоданных
- Сопоставление геоданных по умолчанию

Руководство пользователя

- Ресурсы LogAnalyzer
- Операции с ресурсами
- Создание, переименование, перемещение и удаление папок с ресурсами
- Создание, дублирование, перемещение, редактирование и удаление ресурсов
- Массовое удаление ресурсов
- 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 storage
- Точка назначения, тип eventRouter
- 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
- Фильтры

- Прокси-серверы
- Словари
- Коннекторы
  - Просмотр параметров коннектора
  - Добавление коннектора
  - Параметры коннекторов
    - Коннектор, тип internal
    - Коннектор, тип tcp
    - Коннектор, тип udp
    - 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
  - Предустановленные коннекторы
- Секреты

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
    - Группировка событий
    - Отображение названий вместо идентификаторов
    - Пресеты
    - 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
Формирование SQL-запроса с помощью SQL-функций LogAnalyzer
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
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
Виджет События
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 LogAnalyzer
- Модель данных нормализованного события
- Настройка модели данных нормализованного события из KATA EDR
- Модель данных учетной записи
- События аудита LogAnalyzer
  - Поля событий с общей информацией
  - Пользователь успешно вошел в систему или не смог войти
  - Логин пользователя изменен
  - Роль пользователя изменена
  - 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
  - Токен доступа пользователя изменен
  - Изменен набор пространств для разграничения доступа к событиям
  - Сервис создан
  - Сервис удален
  - Сервис перезагружен
  - Сервис перезапущен
  - Сервис запущен
  - Сервис сопряжен
  - Статус сервиса изменен
  - Индекс партиции удален пользователем
  - Раздел хранилища автоматически удален в связи с истечением срока действия
  - Раздел хранилища автоматически удален или перемещен в связи с превышением объема хранилища
  - Ресурс добавлен
  - Ресурс удален
  - Ресурс обновлен
  - Параметры обновлены
  - Тенант создан
  - Тенант включен
  - Тенант выключен
  - Другие данные тенанта изменены
  - Изменена политика хранения данных после изменения дисков или операция завершилась с ошибкой
  - Словарь успешно обновлен на сервисе или операция завершилась ошибкой
- Отправка тестовых событий в LogAnalyzer

- 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 LogAnalyzer
- Кластер
- Коллектор
- Коннектор
- 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

Список ограничений

Справка Kaspersky LogAnalyzer

Аппаратные и программные требования

- Аппаратные и программные требования

Начало работы

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

Работа в веб-интерфейсе LogAnalyzer

- Руководство администратора
- Руководство пользователя

Дополнительные возможности

- Взаимодействие с внешними системами по API

Лицензирование

- Лицензирование LogAnalyzer

Обращение в Службу технической поддержки

- Способы получения технической поддержки

О программе LogAnalyzer

LogAnalyzer (далее также "программа") – это комплексное программное решение, сочетающее в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности приложений Kaspersky;
- поиск по полученным событиям;
- построение панелей мониторинга и формирование отчетов по полученным событиям.

LogAnalyzer доступна в следующих версиях:

- Базовая (поставляется в составе других решений).
- Коммерческая (поставляется как отдельное решение).

Программа построена на микросервисной архитектуре. Это означает, что вы можете создавать и гибко настраивать микросервисы (далее также "сервисы") под конкретную инфрастурктуру.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в программе на территории США.

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-ansible-installer-<номер сборки>.tar.gz – используется для установки LogAnalyzer без использования Kubernetes. Доступна распределенная установка с Ядром LogAnalyzer в кластере на основе алгоритма Raft.
- kuma-ansible-installer-k8s-<номер сборки>.tar.gz – используется для установки LogAnalyzer 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 LogAnalyzer.

В таблице ниже приведены аппаратные и программные требования к оборудованию для установки компонентов LogAnalyzer, 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 необходимо учитывать не только количество EPS, средний размер события и глубину хранения. При проектировании кластера необходимо учесть нюансы, которые в этой статье для удобства собраны в следующие разделы:

- Дисковая подсистема
- Сетевой интерфейс
- Оперативная память
- Профиль использования

Дисковая подсистема

Основная нагрузка на ClickHouse в LogAnalyzer - это вставки (запись):

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

Разумеется, 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:

1. Использовать DAS (Direct Attached Storage) с NVME или SAS/SATA-интерфейсами, избегая решений класса SAN/NAS.
2. Если узлы кластера ClickHouse развернуты в виртуальной среде, директория /opt/kaspersky/kuma должна быть напрямую смонтирована на дисковый массив. Не следует использовать виртуальные диски.
3. Если есть возможность использовать SSD (SATA/NVME) - это предпочтительный вариант. Любые SSD серверного класса обеспечат большую производительность, чем HDD (даже 15к RPM). Для SSD следует использовать RAID-10 или RAID-0, RAID-0 - при условии использования репликации в ClickHouse.
4. Если использование SSD невозможно, следует применять HDD 15к RPM, SAS, объединенные в RAID-10.
5. Допускается гибридный вариант - горячие данные (например, за последний месяц) хранятся на SSD, а холодные данные - на HDD. Таким образом операции записи всегда будут адресованы SSD-массивам.

6. 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 stripe size был равен 1 МБ. Часто в аппаратных RAID-контроллерах stripe size по умолчанию выставлен в 64 КБ, а максимально доступное значение - 256-512 КБ. Для RAID-10 near-layout более оптимален для записи, а far-layout - для чтения. Это следует учитывать в случае использования гибридного варианта SSD + HDD.

7. Рекомендуемая файловая система - EXT4. Если по какой-либо причине использование этой файловой системы невозможно, допустимо также использование файловой системы XFS. Для любой из этих файловых систем рекомендуется включить опцию монтирования noatime.

Сетевой интерфейс

1. На каждом узле кластера должен быть установлен и соответствующим образом скоммутирован сетевой интерфейс с пропускной способностью не менее 10 Гбит/с. С учетом write amplification и репликации идеальным 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 придерживаться отношения RAM к объему хранимых данных равному 1:100.
Но сколько оперативной памяти потребуется, если на каждом узле предполагается хранить 50 ТБ, ведь зачастую глубина хранения событий определяется требованиями регулятора, и поисковые запросы не выполняются на всю глубину хранения? Поэтому рекомендацию можно трактовать следующим образом: если средняя глубина запроса предполагает сканирование партиций суммарным объемом в 10 ТБ, то потребуется 100 ГБ RAM. Это общая рекомендация, рассчитанная на широкие аналитические запросы.
В общем случае, наличие свободной памяти на сервере положительно влияет на производительность поисковых запросов по наиболее свежим событиям, так как содержимое файлов партиций будет продублировано в Page Cache OS, соответственно, считываться содержимое файлов будет из RAM, 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 вставки). На этапе внедрения KUMA не всегда представляется возможность точно ответить на следующие вопросы:

1. Какие поисковые и аналитические запросы будут выполняться в системе?

2. Какова интенсивность, конкурентность и глубина поисковых запросов?

3. Какова фактическая производительность узлов кластера?

Таким образом эволюция кластера ClickHouse в процессе эксплуатации LogAnalyzer является вполне нормальной практикой. Если в результате увеличения потока EPS или увеличения интенсивности/ресурсоемкости поисковых запросов кластер перестает справляться с нагрузкой, следует либо добавить больше шардов (горизонтальное масштабирование), либо усовершенствовать дисковые подсистемы / CPU / RAM 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.

LogAnalyzer 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 LogAnalyzer	–	–	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 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.
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.

	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Операционные системы	• Ubuntu 22.04 LTS, 24.04 LTS. • Oracle Linux 8.6, 8.7, 8.10, 9.2, 9.3, 9.4, 9.5. • Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 оперативное обновление 1.7.1). • Astra Linux Special Edition РУСБ. 10015-01 (2022-1011SE17MD оперативное обновление 1.7.2.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2022-1110SE17 оперативное обновление 1.7.3). Требуется версия ядра 5.15.0.33 или выше. • Astra Linux Special Edition РУСБ.10015-01 (2023-0630SE17MD срочное оперативное обновление 1.7.4.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2024-0212SE17MD срочное оперативное обновление 1.7.5.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2024-0830SE17 срочное оперативное обновление 1.7.6). • Astra Linux Special Edition РУСБ.10015-01 (2025-0319SE17 срочное оперативное обновление 1.7.7). • Astra Linux Special Edition РУСБ.10015-01 (2025-0114SE18MD срочное оперативное обновление 1.8.1.UU.2). • РЕД ОС 7.3.4, 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 LogAnalyzer, 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 LogAnalyzer в зависимости от уровня EPS, включая требования к хранилищу и рекомендации по масштабированию.

Рекомендуемые конфигурации оборудования и потребление ресурсов LogAnalyzer 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 LogAnalyzer. Один сервер для коллектора. Три выделенных сервера с ролью кипера. Два сервера для хранилища.	Один сервер для Ядра LogAnalyzer. Два сервера для коллектора. 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.	Для Ядра LogAnalyzer, коллектора и кипера требуется от 16 потоков или 16 vCPU и от 64 ГБ оперативной памяти на каждый сервер. 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:

- 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 LogAnalyzer, 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 LogAnalyzer 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.

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 касательно ресурсов для компонента 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 LogAnalyzer вычислительных ресурсов зависят от типа анализируемых событий и от эффективности нормализатора.

Рекомендации экспертов "Лаборатории Касперского" 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 LogAnalyzer рекомендуется устанавливать ClickHouse на аппаратных серверах.

Требования к устройствам для установки агентов

Для передачи данных в коллектор LogAnalyzer 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 версии 8.6, 8.7, 9.2, 9.4, 9.5. • Alma Linux 9.5. • Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 оперативное обновление 1.7.1). • Astra Linux Special Edition РУСБ. 10015-01 (2022-1011SE17MD оперативное обновление 1.7.2.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2022-1110SE17 оперативное обновление 1.7.3). • Astra Linux Special Edition РУСБ.10015-01 (2023-0630SE17MD срочное оперативное обновление 1.7.4.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2025-0319SE17 срочное оперативное обновление 1.7.7). • Astra Linux Special Edition РУСБ.10015-01 (2025-0114SE18MD срочное оперативное обновление 1.8.1.UU.2). • Astra Linux 1.8 x86-64 с установленной библиотекой glibc 2.36 (Debian GLIBC 2.36-9+deb12u7+ci202405171200+astra5). • Astra Linux 1.7 x86-64 с установленной библиотекой glibc 2.28 (Debian GLIBC 2.28-10+deb10u4+ci202407161455+astra12). • 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 транспортами WEC, ETW и WMI

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Агенты LogAnalyzer, установленные на устройствах с операционной системой Windows, могут использовать различные типы транспортов 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 транспорта

Тип транспорта	Максимальная производительность (EPS)	Ограничения со стороны Windows	Ограничения со стороны LogAnalyzer	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 LogAnalyzer 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 LogAnalyzer, установленные на устройствах с операционной системой Linux, могут использовать различные типы транспортов. Аппаратные требования к агентам LogAnalyzer 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 клиентским устройствам для работы с веб-интерфейсом LogAnalyzer

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 LogAnalyzer в Kubernetes

Кластер Kubernetes для развертывания LogAnalyzer 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 LogAnalyzer в Kubernetes представлены в таблице ниже.

Минимальные аппаратные требования к устройствам для установки LogAnalyzer 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	От 1 ТБ в директории /opt/ От 32 ГБ в директории /var/lib/
Пропускная способность сети	10 Гбит/с	10 Гбит/с	10 Гбит/с

Интерфейс LogAnalyzer

Работа с программой осуществляется через веб-интерфейс.

Окно веб-интерфейса программы содержит следующие элементы:

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

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

Во время работы с веб-интерфейсом программы 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 LogAnalyzer 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 LogAnalyzer, 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.
- Добавьте в общие исключения и в исключения для проверки по требованию следующие директории:

  a. На сервере Ядра LogAnalyzer:

  - /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 коллекторов:

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

  d. Папки с журналами для каждого сервиса.

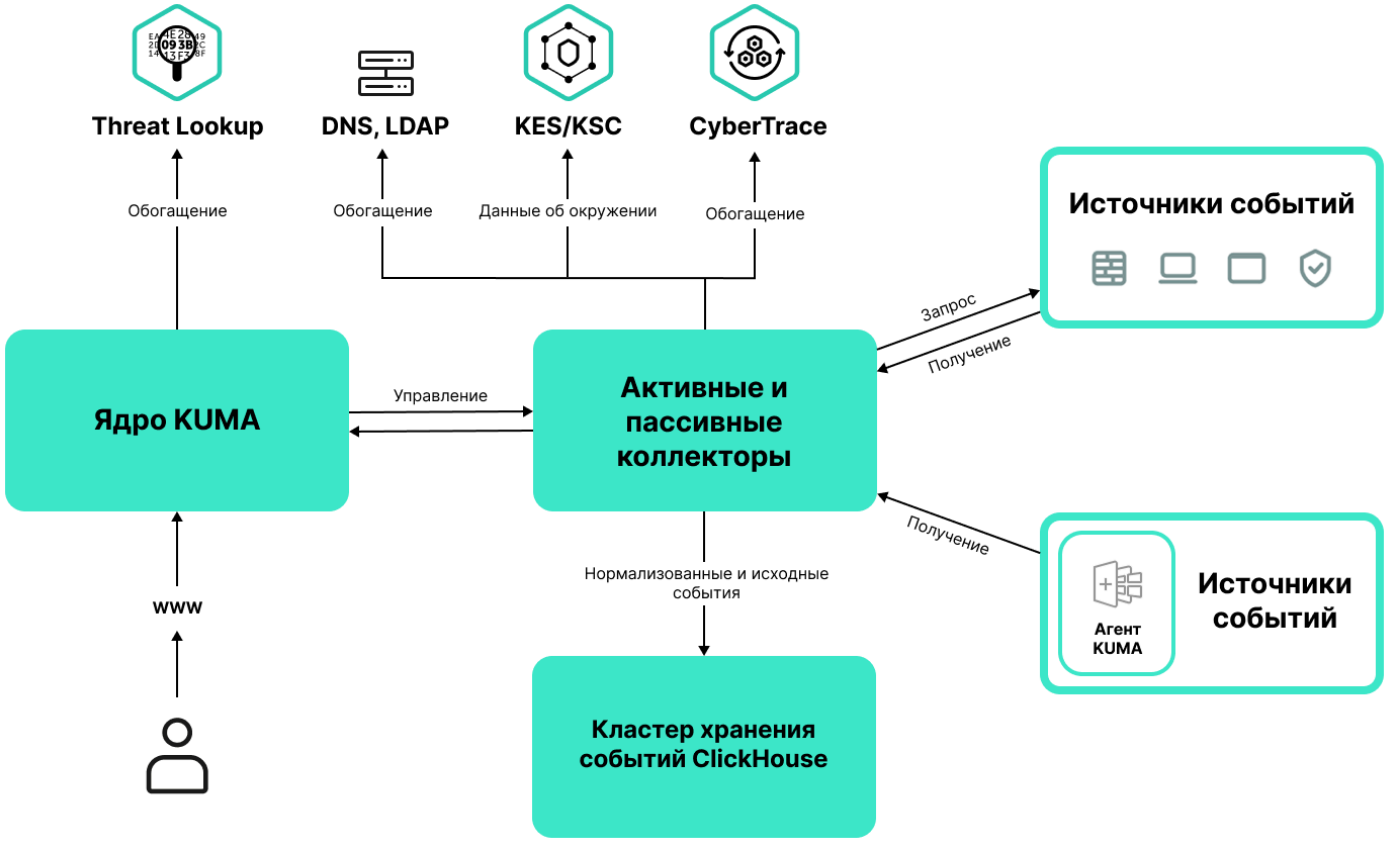
Подробнее об исключениях из проверки см. онлайн-справку Kaspersky Endpoint Security для Linux.

Архитектура программы

Стандартная установка программы 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 LogAnalyzer.
- 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.
- *Хранилище*, в котором содержатся нормализованные события.

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 LogAnalyzer

Ядро

Ядро – это центральный компонент LogAnalyzer, 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) программы, а также интегрировать в систему необходимое программное обеспечение;
- централизованно управлять сервисами и учетными записями пользователей программы;
- визуально представлять статистические данные о работе программы.

Коллектор

Коллектор – это компонент программы, который получает сообщения из источников событий, обрабатывает их и передает в хранилище и/или сторонние сервисы.

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.

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 программе доступны следующие типы коннекторов:

   - tcp;
   - udp;
   - 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 программе доступны следующие нормализаторы:

   - JSON;
   - CEF;
   - Regexp;
   - Syslog (как для RFC3164 и RFC5424);
   - CSV;
   - Ключ-значение;
   - XML;
   - 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 программе представлены следующие источники обогащения:

- константы;
- словари (доступно только в коммерческой версии LogAnalyzer);
- cybertrace (доступно только в коммерческой версии LogAnalyzer);
- cybertrace-http (доступно только в коммерческой версии LogAnalyzer);
- dns (доступно только в коммерческой версии LogAnalyzer);
- события;
- шаблоны;
- данные о часовых поясах;
- геоданные;
- проверка DLL Hijacking.

Правила преобразования позволяют преобразовать содержимое поля события в соответствии с заданными условиями. В программе 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. 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.

Хранилище

Хранилище LogAnalyzer используется для хранения нормализованных событий таким образом, чтобы к ним обеспечивался быстрый и бесперебойный доступ из LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer.

О тенантах

В LogAnalyzer действует режим мультитенантности, при котором один экземпляр программы LogAnalyzer, 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 LogAnalyzer.

По умолчанию в LogAnalyzer 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 LogAnalyzer 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.

О событиях

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 LogAnalyzer.

LogAnalyzer 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 хранилища для хранения.

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

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

   В программе представлены следующие нормализаторы:

   - JSON
   - CEF
   - Regexp
   - Syslog (как для RFC3164 и RFC5424)
   - CSV/TSV
   - Ключ-значение
   - XML
   - SQL

   По завершении этого этапа нормализованные события можно использовать для анализа.

3. Точка назначения. После обработки события коллектором оно готово к пересылке в хранилище LogAnalyzer.

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

4. Событие мониторинга. Такие события используются для отслеживания изменений в количестве данных, поступающих в LogAnalyzer.

Об активах

Активы – это сетевые устройства, зарегистрированные в LogAnalyzer. Активы генерируют сетевой трафик при отправке и получении данных. Программа LogAnalyzer может быть настроена 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).

О ресурсах

Ресурсы – это компоненты LogAnalyzer, 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 LogAnalyzer.

О сервисах

Сервисы – это основные компоненты LogAnalyzer, 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 LogAnalyzer на основе набора ресурсов для сервисов.
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система LogAnalyzer, 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.

Об агентах

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

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.

Лицензирование программы

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

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Перейти в папку с распакованным установщиком и прочитать текстовый файл ./roles/kuma/files/LICENSE
- Перейти в папку 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 LogAnalyzer - таким как Ядро, коллектор, 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 папке /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 kuma и выполнить следующую команду, чтобы вывести на экран текст лицензионного соглашения:

  ./kuma license --show

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Лицензия предоставляется при приобретении программы. Поведение LogAnalyzer в случае отсутствия лицензии:

- По истечении срока действия лицензии LogAnalyzer 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 LogAnalyzer прекращают принимать и обрабатывать новые события сразу. Старые события доступны. Также невозможно создавать и редактировать ресурсы, создавать и запускать сервисы.

Чтобы продолжить использование LogAnalyzer 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 программе, которую 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 программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу, применив *файл ключа*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

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

Лицензионный ключ может быть активным и резервным.

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

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, 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 программу.

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

Чтобы активировать программу 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 лицензионном коде

Лицензионный код – это уникальная последовательность из двадцати латинских букв и цифр, которая позволяет активировать программу. Вы получаете лицензионный код от "Лаборатория Касперского" по указанному вами адресу электронной почты после приобретения LogAnalyzer.

При активации лицензионным кодом с сервера Ядра требуется постоянный доступ в интернет. Чтобы активировать программу с помощью лицензионного кода требуется подключение к серверу активации "Лаборатории Касперского":

https://activation-v2.kaspersky.com:443

В случае закрытой инфраструктуры вы можете указать прокси-сервер.

Если лицензионный код был случайно удален, вы можете получить его повторно, для этого вам нужно обратиться к продавцу лицензии.

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

В веб-интерфейсе программы отображаются параметры настройки в зависимости от функционала, который покрывает лицензия.

Если вы хотите использовать лицензионный код для активации LogAnalyzer, в разделе **Параметры** → **Лицензия** в раскрывающемся списке **Тип активации** выберите **Активация ключом**.

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

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

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

Предоставление данных в Kaspersky LogAnalyzer

Данные, передаваемые третьим сторонам

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

Данные, обрабатываемые локально

Kaspersky LogAnalyzer (далее "LogAnalyzer" или "программа") – это комплексное программное решение, сочетающее в себе следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;
- поиск по полученным событиям;
- построение отчетов и дашбордов для мониторинга состояния инфраструктуры заказчика;
- мониторинг источников событий.

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

- Данные, содержащиеся в событиях от настроенных источников.

  В коллекторе настраивается источник событий, с которого будут передаваться события, формируются события и передаются далее в другие сервисы программы. В некоторых случаях первой точкой приема событий может стать сервис агента, который передает события от источника в коллектор. Дополнительно можно настроить сохранение адреса или имя хоста сервера-агрегатора событий.

- Данные, необходимые для интеграции LogAnalyzer с другими приложениями (Kaspersky Threat Lookup, Kaspersky CyberTrace).

  Это могут быть сертификаты, токены, URL или данные учетной записи для установки безопасного соединения с другим приложением, а также другие данные для обеспечения основной функциональности LogAnalyzer, например, адрес электронной почты. Пользователь вводит эти данные в веб-интерфейсе LogAnalyzer.

- 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 веб-интерфейсе LogAnalyzer.

- Параметры профиля пользователя:

  - Роль пользователя в LogAnalyzer. Пользователь может видеть назначенную ему роль(-и).

  - Язык локализации, параметры уведомлений, отображение непечатаемых символов.

    Пользователь вводит эти данные в веб-интерфейсе LogAnalyzer.

  - 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 веб-интерфейса LogAnalyzer.

- Данные для доменной аутентификации пользователей в LogAnalyzer:
  - 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 LogAnalyzer 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.

  LogAnalyzer автоматически фиксирует события аудита.
- Журнал событий KUMA.

  Пользователь может включить ведение расширенных записей журналов в веб-интерфейсе LogAnalyzer. 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 LogAnalyzer.
- Любые данные, которые пользователь вводит в веб-интерфейсе LogAnalyzer.

Перечисленные выше данные могут попасть в LogAnalyzer следующими способами:

- Пользователь вводит данные в веб-интерфейсе LogAnalyzer.
- Сервисы LogAnalyzer (агент или коллектор) получают данные при настроенном пользователем подключении к источникам событий.
- Через REST API LogAnalyzer.

Перечисленные данные хранятся в базе данных LogAnalyzer (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 LogAnalyzer, включая файлы журналов, создаваемые установщиком и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов LogAnalyzer 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 LogAnalyzer.

"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 в веб-интерфейс программы

В веб-интерфейсе LogAnalyzer можно добавить лицензионный ключ приложения. Если вы активируете приложение с помощью файла ключа, то лицензионных ключей может быть два – активный и резервный. Если же вы используете код активации, лицензионный ключ будет один. В LogAnalyzer 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 LogAnalyzer 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 лимита EPS этого лицензионного ключа будет автоматически вычтено из суммарного значения EPS объединенной лицензии. Соответственно, при добавлении нового активного лицензионного ключа в объединенную лицензию значение лимита 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, LogAnalyzer отображает предупреждение и добавит такой лицензионный ключ только после вашего подтверждения.

- Объединенная лицензия может включать до 50 активных ключей.

Только пользователи с ролью администратора могут добавлять лицензионные ключи.

Добавление новой группы лицензий

Чтобы добавить новую группу лицензий:

1. Откройте веб-интерфейс LogAnalyzer и выберите раздел **Параметры** → **Другое** → **Лицензия**.

   Откроется окно со списком добавленных групп лицензий.

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

3. В открывшемся окне введите имя новой группы лицензий.
4. Выберите способ добавления лицензионного ключа:
   - С помощью кода активации.
     1. Укажите код активации.
     2. Если в компании при подключении к интернету используется прокси-сервер, укажите его параметры. Для активации приложения потребуется подключение к интернету.
   - С помощью файла ключа.
     1. В разделе **Активный лицензионный ключ** нажмите на кнопку **Загрузить**, затем выберите файл ключа (файл с расширением KEY).
     2. В разделе **Резервный лицензионный ключ** аналогичным образом добавьте резервный лицензионный ключ.
5. Нажмите на кнопку **Активировать**.

Группа лицензий добавлена в список, приложение активировано.

Добавление резервного лицензионного ключа

Чтобы добавить резервный лицензионный ключ в группу лицензий:

1. Откройте веб-интерфейс LogAnalyzer и выберите раздел **Параметры** → **Другое** → **Лицензия**.

   Откроется окно со списком добавленных групп лицензий.
2. Нажмите на имя требуемой 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 **Активировать**.

Замена активного лицензионного ключа

Если вы хотите добавить активный лицензионный ключ вместо уже добавленного ключа, сначала удалите текущий лицензионный ключ. Затем добавьте новый лицензионный ключ.

Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы

В веб-интерфейсе LogAnalyzer можно просмотреть информацию о добавленном лицензионном ключе. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензия**.

Только пользователи с ролью администратора могут просматривать информацию о лицензии.

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

- **Истекает** – дата истечения срока действия лицензионного ключа.
- **Осталось дней** – количество дней до истечения срока действия лицензии.
- **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 LogAnalyzer считает количество событий после их обработки коллектором (после фильтрации и агрегации на выходе из коллектора) до среднего EPS за час, а затем – за сутки.
- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
- **Компания** – название компании, купившей лицензию.
- **Имя клиента** – имя клиента, который приобрел лицензию.
- **Модули** – модули, доступные для лицензии.

Дополнительные параметры для лицензий SMART I и SMART II

Для лицензий SMART I и SMART II доступны следующие параметры в дополнение к указанным выше:

- **Текущее EPS за сутки** – текущее среднее количество событий за сутки, которое обрабатывает LogAnalyzer.
- **Текущее EPS за час** – текущее среднее количество событий за час, которое обрабатывает LogAnalyzer.

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.

Удаление лицензионного ключа в веб-интерфейсе программы

Вы можете удалить добавленный лицензионный ключ из LogAnalyzer (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 редактировать ресурсы, создавать и запускать сервисы. Эта работа возобновится при добавлении лицензионного ключа.

Только пользователи с ролью администратора могут удалять лицензионные ключи.

Чтобы удалить лицензионный ключ:

1. Откройте веб-интерфейс LogAnalyzer и выберите раздел **Параметры** → **Лицензия**.

   Откроется окно с условиями лицензии LogAnalyzer.

2. Нажмите на значок на лицензионном ключе, который требуется удалить.

   Откроется окно подтверждения.

3. Подтвердите удаление лицензионного ключа.

Лицензионный ключ удален из программы.

Руководство администратора

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

Установка и удаление LogAnalyzer

Внимание! Установка приложения в отказоустойчивой конфигурации, включая установку в кластере Kubernetes или кластере Raft, нарушает сертифицированную конфигурацию приложения.

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 LogAnalyzer в кластере на основе алгоритма Raft (далее — "в кластере Raft").

- **kuma-ansible-installer-<номер сборки>-environment.tar.gz** содержит компоненты для установки библиотеки для подключения к СУБД Oracle, Chromium, а также компоненты автоматизации настройки и развертывания LogAnalyzer.

- **kuma-ansible-installer-k8s-<номер сборки>.tar.gz** (не входит в комплект поставки сертифицированной версии продукта) 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

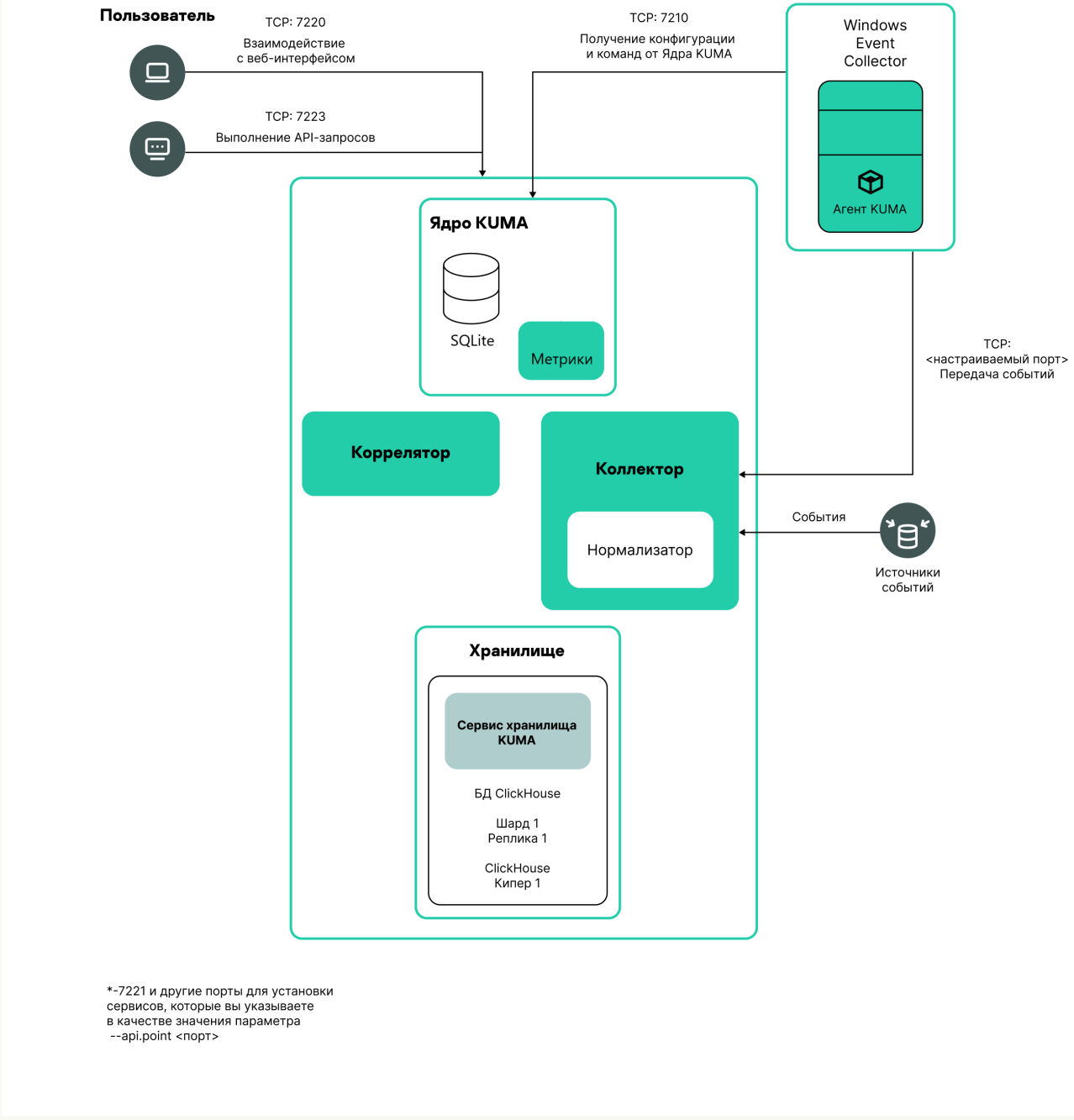
LogAnalyzer размещает свои файлы в папке /opt, поэтому мы рекомендуем сделать /opt отдельным разделом и выделить под него все дисковое пространство, за исключением 16 ГБ для операционной системы.

Установка LogAnalyzer 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



Установка на одном сервере

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_user: root
  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
```

Вы можете установить все компоненты LogAnalyzer 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

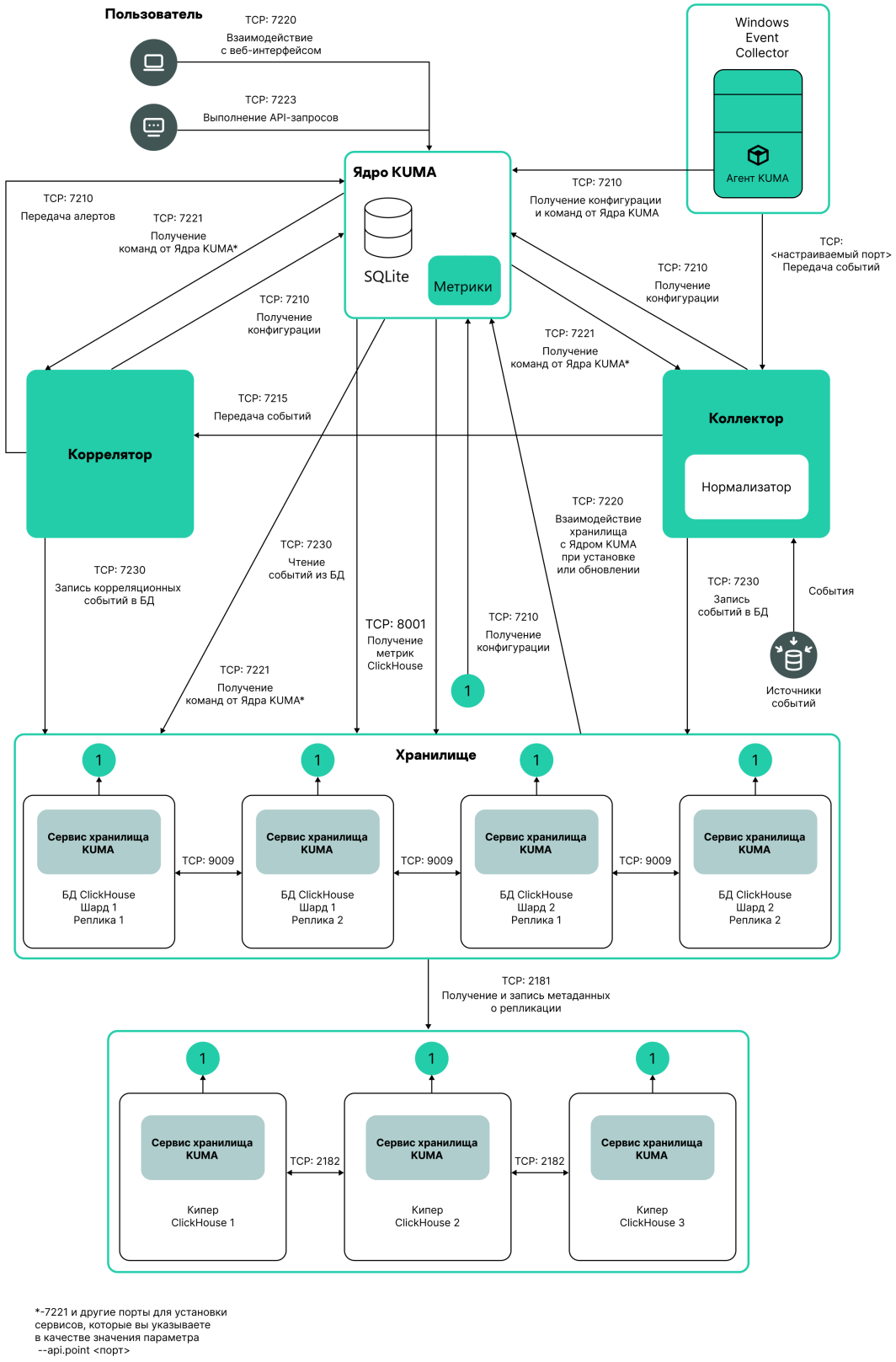


Схема распределенной установки

Пример файла инвентаря для схемы распределенной установки

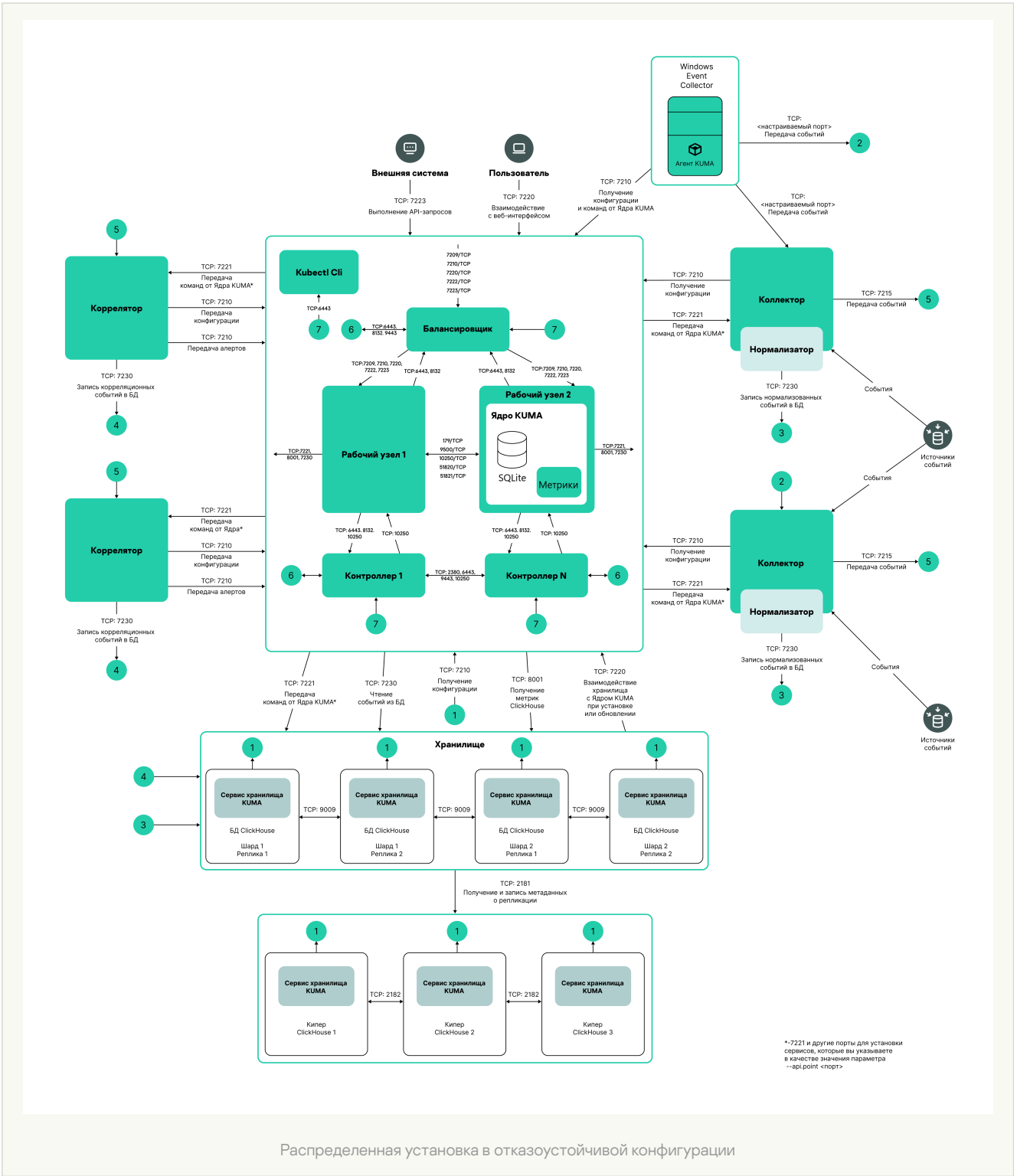
```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          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 LogAnalyzer на разных серверах: конфигурацию для распределенной установки вы можете описать в файле инвентаря distributed.inventory.yml.

- Установка в отказоустойчивой конфигурации:
  - Распределенная установка с Ядром LogAnalyzer в кластере Kubernetes

    Схема распределенной установки с Ядром LogAnalyzer в кластере Kubernetes



Распределенная установка в отказоустойчивой конфигурации

Пример файла инвентаря для схемы распределенной установки с Ядром LogAnalyzer 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 LogAnalyzer в кластере Kubernetes для обеспечения отказоустойчивости. Используйте файл инвентаря k0s.inventory.yml для описания конфигурации.

- Распределенная установка с Ядром LogAnalyzer в кластере Raft

  Схема распределенной установки с Ядром LogAnalyzer в кластере Raft

  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 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 LogAnalyzer в кластере Raft для репликации данных и обеспечения отказоустойчивости в распределенной системе. Используйте файл инвентаря distributed.inventory.yml для описания конфигурации.

Требования к установке программы

Общие требования к установке программы

Вы можете установить программу 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 программы убедитесь, что выполнены следующие условия:

- Серверы, предназначенные для установки компонентов, соответствуют аппаратным и программным требованиям.
- Порты, которые LogAnalyzer займет при установке, доступны.
- Адресация компонентов LogAnalyzer осуществляется по полному доменному имени FQDN хоста в формате hostname.example.com. Перед установкой программы убедитесь, что в поле `Static hostname` возвращается правильное имя FQDN хоста. Для этого выполните команду:

  ```
  hostnamectl status
  ```

- Имя сервера, на котором запускается установщик, отличается от `localhost` или `localhost.<домен>`.
- Имя сервера, на котором будет установлено Ядро LogAnalyzer, не начинается с цифры.
- Настроена синхронизация времени на всех серверах с сервисами LogAnalyzer по протоколу Network Time Protocol (NTP).

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.
Система управления пакетами	pip3.	pip3.	pip3.	pip3.	pip3.

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	МосОС

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.
		Вы можете установить пакеты с помощью команды:
		`apt install python3-apt curl libcurl4`
			• python3-apt.
			• curl.
			• libcurl4.
			Вы можете установить пакеты с помощью команды:
			`apt install python3-apt curl libcurl4`
				• netaddr.
				• firewalld.
				Вы можете установить пакеты с помощью следующих команд:
				`pip3 install netaddr`
				`dnf install firewalld`
					• python3-rpm
					Вы можете установить пакет с помощью следующих команд:
					`zypper refresh`
					`zypper install python3-rpm`

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 LogAnalyzer, 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.

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	МосОС

Пакеты, которые нужно установить на устройстве с Ядром LogAnalyzer 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:
			`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`
				• 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.

Уровень прав пользователя, необходимый для установки программы	Нет значения.	Вам нужно присвоить необходимый уровень прав пользователю, под которым вы собираетесь устанавливать программу, с помощью команды: `sudo pdpl-user -i 63 < имя пользователя, под которым вы собираетесь устанавливать программу >`	Нет значения.	Нет значения.	Нет значения.

Обновление с операционной системы Oracle Linux 8.x до Oracle Linux 9.x

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

1. Отключите сервисы LogAnalyzer на хостах, где сервисы установлены, с помощью следующих команд:
   - `sudo systemctl disable kuma-collector-<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-metrics-<идентификатор сервиса metrics>.service`
   - `sudo systemctl enable kuma-vmalert.service`
4. Перезагрузите хосты.

В результате обновление выполнено.

Порты, используемые LogAnalyzer при установке

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

Перед установкой Ядра на устройстве убедитесь, что следующие порты свободны:

- 7227: используется сервисом Метрики.
- 8880: используется VMalert.

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

Сетевые порты, используемые для взаимодействия компонентов LogAnalyzer

Протокол	Порт	Направление	Назначение подключения
HTTPS	7222	От клиента LogAnalyzer к серверу с компонентом Ядро LogAnalyzer.	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 LogAnalyzer на сервер Ядра LogAnalyzer.	Получение конфигурации LogAnalyzer от сервера Ядра LogAnalyzer.
TCP	7220	• От клиента LogAnalyzer к серверу с компонентом Ядро LogAnalyzer. • От хостов хранилищ к серверу с компонентом Ядро KUMA во время установки или обновления.	• Доступ пользователей к веб-интерфейсу LogAnalyzer. • 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 LogAnalyzer к сервисам LogAnalyzer.	Администрирование сервисов из веб-интерфейса LogAnalyzer.
TCP	7223	К серверу Ядра LogAnalyzer.	Порт, используемый по умолчанию для API-запросов.
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 LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer в отказоустойчивой конфигурации

Источник	Назначение	Порт назначения	Тип
Внешние сервисы LogAnalyzer	Балансировщик нагрузки	7209	TCP
Внешние сервисы LogAnalyzer	Балансировщик нагрузки	7210	TCP
Внешние сервисы LogAnalyzer	Балансировщик нагрузки	7220	TCP
Внешние сервисы LogAnalyzer	Балансировщик нагрузки	7222	TCP
Внешние сервисы LogAnalyzer	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 LogAnalyzer	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 LogAnalyzer	Рабочий узел	7209	TCP
Внешние сервисы LogAnalyzer	Рабочий узел	7210	TCP
Внешние сервисы LogAnalyzer	Рабочий узел	7220	TCP
Внешние сервисы LogAnalyzer	Рабочий узел	7222	TCP
Внешние сервисы LogAnalyzer	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

Источник	Назначение	Порт назначения	Тип
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 LogAnalyzer вы можете скачать следующие CA-сертификаты:

- CA-сертификат REST API.

  Сертификат требуется для проверки подлинности API-сервера, обслуживающего публичное API LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** необходимо выбрать сервис, выбрать в контекстном меню **Сбросить сертификат** и удалить прежний сертификат в директории установки сервиса. LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 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 LogAnalyzer, чтобы применить новые CA-сертификаты.

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

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

   - Для LogAnalyzer с Ядром в кластере Kubernetes чтобы перезапустить Ядро LogAnalyzer, 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 LogAnalyzer с использованием команды, поскольку перезапуск Ядра LogAnalyzer через интерфейс LogAnalyzer влияет на перезапуск только контейнера Ядра LogAnalyzer, 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 LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer примет файл ключа.

3. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer:

   ```
   systemctl restart kuma-core
   ```

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

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 LogAnalyzer в файле инвентаря, а установщик использует эти значения при развертывании, обновлении и удалении программы. 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 LogAnalyzer 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 LogAnalyzer без использования кластера Kubernetes, расширения установки "все в одном" до распределенной и для обновления LogAnalyzer.

- expand.inventory.yml.template – используется в ряде сценариев изменения конфигурации: для добавления серверов коллекторов, 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 LogAnalyzer в кластер Kubernetes.

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

Параметры конфигурации LogAnalyzer 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 LogAnalyzer 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. • `local` – подключение к удаленным хостам не производится.
`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.

Переменная	Описание
`ansible_become`	Переменная, определяющая, требуется ли повышать привилегии пользователя, от имени которого осуществляется установка компонентов LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer 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`.
`need_transfer`	Переменная, определяющая, требуется ли переносить Ядро LogAnalyzer в новый кластер Kubernetes. Вам нужно указать эту переменную, только если для переменной `deploy_to_k8s` вы указали значение `true`. Возможные значения: • `false` – LogAnalyzer требуется установить или обновить в кластере Kubernetes. • `true` – Ядро LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer. Это значение указано во всех шаблонах файла инвентаря. • `true` – предустановленные сервисы создаются при установке LogAnalyzer. Если вы не укажете эту переменную, по умолчанию будет использовано значение `false`.

Переменная	Описание
`low_resources`	Переменная, определяющая, устанавливается ли KUMA в окружениях с ограниченными вычислительными ресурсами. Эта переменная отсутствует во всех шаблонах файла инвентаря. Возможные значения: • `false` – LogAnalyzer 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` – LogAnalyzer устанавливается в окружениях с ограниченными вычислительными ресурсами. В этом случае минимальный объем директории для установки Ядра LogAnalyzer 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 LogAnalyzer для установки в кластере Kubernetes. Если значение переменной не задано, то для размера тома Ядра LogAnalyzer при установке будут принятые следующие значения по умолчанию: • Если `low_resources=false`, размер тома по умолчанию - 512Gi. • 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 LogAnalyzer 3.4 в новый том метрик в LogAnalyzer 4.0. Значение по умолчанию: 120m. Суффикс m обязателен для указания.

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 LogAnalyzer.
    - `ansible_port` – переменная для указания нестандартных портов для SSH в ходе установки. Следует указывать для каждого хоста в файле инвентаря, даже если на всех хостах используются одинаковые порты. Необязательный параметр.
    - `raft_node_addr` – адрес, который будет использоваться для кластера узлов с сервисом Ядра LogAnalyzer, должен быть публичным и известным для других узлов. После того, как Ядро LogAnalyzer 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 LogAnalyzer, а <порт> - 7209. Параметр `raft_node_addr` следует задавать вместе с параметром `raft_node_listen на каждом сервере с Ядром LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer`. Необязательный параметр.
  - `kuma_core_peers` – параметры дополнительных Ядер LogAnalyzer. Установщик подготавливает серверы, перечисленные в группе `kuma_core_peers`, для последующей установки дополнительных сервисов Ядра LogAnalyzer. 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 LogAnalyzer. На каждом сервере в группе `kuma_core_peers` допускается установка только одного сервиса Ядра LogAnalyzer.

    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 LogAnalyzer. 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 LogAnalyzer. Сервисы Ядра LogAnalyzer на них не устанавливаются. Вы можете позднее создать дополнительные сервисы Ядра LogAnalyzer 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 нём только группу kuma_core_peers. После запуска установщика expand.sh с файлом инвентаря expand.inventory.yml нужно вручную создать в веб-интерфейсе сервисы Ядра LogAnalyzer 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 LogAnalyzer.	Выполняется обычное расширение установки.

- `raft_node_addr` – адрес, который будет использоваться для кластера узлов с сервисом Ядра LogAnalyzer, должен быть публичным и известным для других узлов. После того, как Ядро LogAnalyzer 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 LogAnalyzer, а <порт> - 7209. Параметр `raft_node_addr` следует задавать вместе с параметром `raft_node_listen` на каждом сервере с Ядром LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer`. Необязательный параметр.

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

  - `ansible_port` – переменная для указания нестандартных портов для SSH в ходе установки. Следует указывать для каждого хоста в файле инвентаря, даже если на всех хостах используются одинаковые порты. Необязательный параметр.

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

  - `ansible_port` – переменная для указания нестандартных портов для SSH в ходе установки. Следует указывать для каждого хоста в файле инвентаря, даже если на всех хостах используются одинаковые порты. Необязательный параметр.

  - `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 LogAnalyzer. В остальных случаях используются идентификаторы шарда, реплики и кипера, которые вы указали в веб-интерфейсе LogAnalyzer при создании набора ресурсов для хранилища.

Блок kuma_k0s

В этом блоке вы можете указать параметры кластера Kubernetes, использование которого обеспечивает отказоустойчивость LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer размещается на контроллере, выключение контроллера приведет к полной потере доступа к Ядру LogAnalyzer.

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"`.	

`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 LogAnalyzer на одном сервере, выполните следующие шаги:

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

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 программы. С помощью single.inventory.yml установщик развернет LogAnalyzer.

3. Установите программу.

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

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

Подготовка файла инвентаря single.inventory.yml

Установка, обновление и удаление компонентов LogAnalyzer производится из папки с распакованным установщиком с помощью инструмента Ansible® и созданного пользователем *файла инвентаря* в формате YML с перечнем хостов компонентов LogAnalyzer и других параметров. Если вы хотите установить все компоненты LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer.

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

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

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_user: root
  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
```

Установка программы на одном сервере

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

Чтобы установить LogAnalyzer на одном сервере:

1. Скачайте на сервер дистрибутив LogAnalyzer 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 приложения, который вы планируете использовать, выберите один из вариантов:

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

     > Активация приложения с помощью лицензионного кода доступна только для LogAnalyzer 3.4 и более поздних версий. Для более ранних версий LogAnalyzer используется активация приложения 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, программа не будет установлена.

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

   - Если вы планируете использовать активацию приложения 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 LogAnalyzer, все заданные в файле инвентаря сервисы и OOTB-ресурсы. Если в файле инвентаря был задан параметр example_services=true, демонстрационные сервисы будут установлены.

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

     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 LogAnalyzer и в строке браузера введите адрес веб-интерфейса LogAnalyzer, а затем на странице входа введите учетные данные.

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

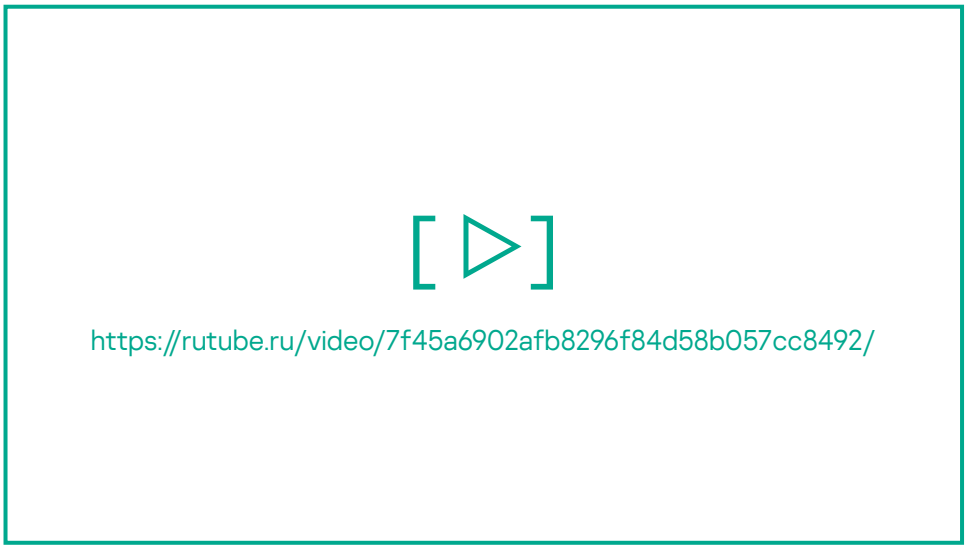
   Учетные данные для входа по умолчанию:
   - логин – `admin`
   - пароль – `mustB3Ch@ng3d!`

   После первого входа измените пароль учетной записи admin

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

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

Установку можно расширить до распределенной.



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

Распределенная установка

Распределенная установка LogAnalyzer происходит в несколько этапов:

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

2. Подготовка контрольной машины.

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

3. Подготовка целевых машин.

   На целевые машины устанавливаются компоненты программы.

4. Подготовка файла инвентаря distributed.inventory.yml.

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы. С помощью этого файла инвентаря установщик развернет LogAnalyzer.

5. Установка программы.

   Установите программу и выполните вход в веб-интерфейс.

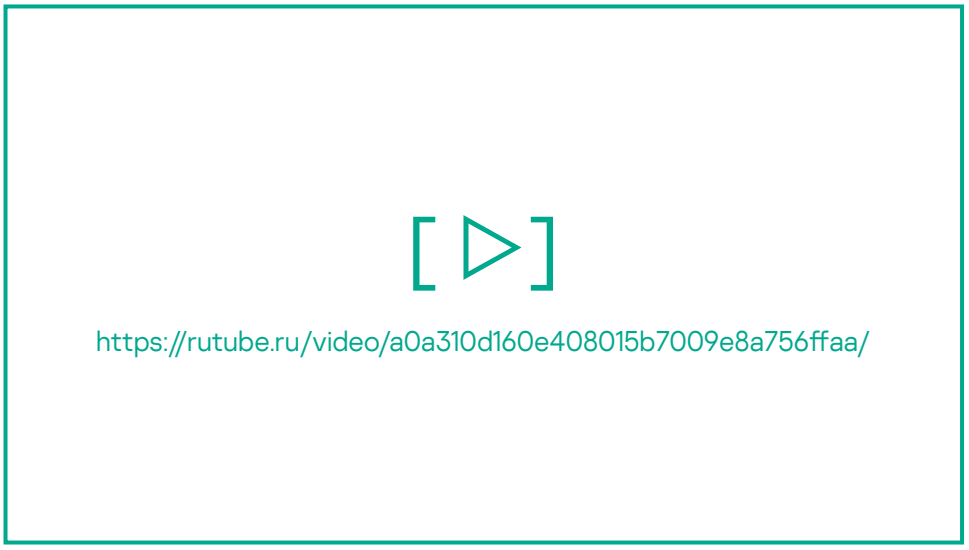
6. Создание сервисов.

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

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

   > При развертывании нескольких сервисов LogAnalyzer 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 LogAnalyzer на сертификат своей компании.



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

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки LogAnalyzer:

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

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 LogAnalyzer.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов LogAnalyzer:

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 LogAnalyzer после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами программы.
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 LogAnalyzer.
4. Чтобы получить имя хоста, которое потребуется указать при установке LogAnalyzer, 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 LogAnalyzer.

Подготовка файла инвентаря distributed.inventory.yml

Чтобы создать файл инвентаря distributed.inventory.yml:

1. Перейдите в директорию установщика LogAnalyzer, 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 программы. С его помощью вы можете дополнить систему компонентами или удалить LogAnalyzer.

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 программы в распределенной конфигурации

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

Чтобы установить LogAnalyzer:

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

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

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

   - Для активации программы 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 программы 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_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:
          ansible_port: 2222
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ansible_port: 2223
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ansible_port: 2224
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ansible_port: 2225
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ansible_port: 2226
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ansible_port: 2227
```

```
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ansible_port: 2228
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

5. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, программа не будет установлена.

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

   - Если вы активируете программу 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 LogAnalyzer, все заданные в файле инвентаря сервисы и OOTB-ресурсы.

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

     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 LogAnalyzer и в строке браузера введите адрес веб-интерфейса LogAnalyzer, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса LogAnalyzer – `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 LogAnalyzer установлены и выполнен вход в веб-интерфейс.

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

Распределенная установка с Ядром LogAnalyzer в кластере Kubernetes

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

Для установки LogAnalyzer 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 LogAnalyzer в кластер Kubernetes можно следующими способами:

- Установить LogAnalyzer в кластере Kubernetes.
- Перенести Ядро существующей установки LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

Для эффективной работы Ядра LogAnalyzer в Kubernetes необходимо выделить 3 обособленных узла с единственной ролью контроллера. Это позволит обеспечить отказоустойчивость самого кластера Kubernetes и гарантировать, что рабочая нагрузка - процессы LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer с помощью программы Kaspersky Endpoint Security for Linux, вам нужно сначала установить LogAnalyzer в кластере Kubernetes и только потом разворачивать Kaspersky Endpoint Security for Linux. При обновлении или удалении LogAnalyzer вам нужно предварительно остановить Kaspersky Endpoint Security for Linux с помощью команды:

```
systemctl stop kesl
```

При установке LogAnalyzer в отказоустойчивом варианте должны выполняться следующие требования:

- Общие требования к установке программы.
- 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 LogAnalyzer, 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. Разделы `upstream` формируются динамически и содержат IP-адреса контроллеров кластера Kubernetes (в примере – 10.0.0.2-4 в разделах `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 LogAnalyzer.
- На сервере балансировщика нагрузки nginx в операционной системе не включен модуль SELinux.
- На хостах установлены пакеты tar, systemctl.

При установке LogAnalyzer 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 LogAnalyzer в кластере Kubernetes

Распределенная установка LogAnalyzer происходит в несколько этапов:

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

2. Подготовка контрольной машины.

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

3. Подготовка целевых машин.

   На целевые машины устанавливаются компоненты программы.

4. Подготовка файла инвентаря k0s.inventory.yml.

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы. С помощью этого файла инвентаря установщик развернет LogAnalyzer.

5. Установка программы.

   Установите программу и войдите в веб-интерфейс.

6. Создание сервисов.

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

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

   > При развертывании нескольких сервисов LogAnalyzer 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 LogAnalyzer на сертификат своей компании.

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки LogAnalyzer:

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

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 LogAnalyzer.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов LogAnalyzer:

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 LogAnalyzer после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами программы.

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 LogAnalyzer, 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 LogAnalyzer.

Подготовка файла инвентаря k0s.inventory.yml

Чтобы создать файл инвентаря k0s.inventory.yml:

1. Перейдите в директорию установщика LogAnalyzer, 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 LogAnalyzer в кластере Kubernetes с 3 контроллерами, 2 рабочими узлами и 1 балансировщиком

```
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_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 LogAnalyzer 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 программы. 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 программы. С его помощью вы можете дополнить систему компонентами или удалить KUMA.

Установка программы в отказоустойчивой конфигурации

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

Чтобы установить LogAnalyzer:

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

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

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

   - Если вы планируете использовать активацию приложения 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 приложения с помощью лицензионного кода, 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, программа не будет установлена.

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

   - Если вы планируете использовать активацию программы 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 LogAnalyzer, все заданные в файле инвентаря сервисы и OOTB-ресурсы.

   - Если вы планируете использовать активацию приложения с помощью лицензионного кода, или планируете предоставить файл ключа позднее, в результате запуска установщика с файлом инвентаря k0s.inventory.yml будет установлено только Ядро LogAnalyzer.

     Чтобы установить сервисы, в консоли командной строки укажите лицензионный код. 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 LogAnalyzer и в строке браузера введите адрес веб-интерфейса LogAnalyzer, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса LogAnalyzer – `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 LogAnalyzer установлены и выполнен вход в веб-интерфейс.

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

Перенос Ядра LogAnalyzer в новый кластер Kubernetes

Чтобы перенести Ядро LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

```
cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

```
cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
```

11. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer при различных сценариях

Доступность Ядра LogAnalyzer при различных сценариях:

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

  Доступ к веб-интерфейсу LogAnalyzer пропадает. Через 6 минут Kubernetes инициирует перенос контейнера с Ядром на работающий узел кластера. После завершения развертывания, которое занимает менее одной минуты, веб-интерфейс LogAnalyzer 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 LogAnalyzer, на котором в этот момент не развернут сервис Ядра.**

  Доступ к веб-интерфейсу LogAnalyzer не пропадает по URL, в которых используется FQDN балансировщика. Сетевое хранилище создает реплику работающего дискового тома Ядра на других работающих узлах. При доступе к LogAnalyzer 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 LogAnalyzer 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
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 LogAnalyzer пропадает. Если утеряны все реплики, будет потеряна информация.

Управление Kubernetes и доступ к LogAnalyzer

При установке LogAnalyzer 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 LogAnalyzer. Например, для просмотра нагрузки на рабочие узлы можно использовать команду:

```
k0s kubectl top nodes
```

Доступ к Ядру LogAnalyzer

Доступ к Ядру LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, 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).

Распределенная установка с Ядром LogAnalyzer в кластере Raft

Распределенная установка LogAnalyzer с несколькими сервисами Ядра LogAnalyzer 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 LogAnalyzer обеспечивает не только отказоустойчивость, но и горизонтальное масштабирование. Допустимо развертывать только нечетное количество сервисов Ядра LogAnalyzer.

При необходимости вы можете выполнить следующие действия:

- Выполнить распределенную установку с Ядром LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра LogAnalyzer в веб-интерфейсе и последовательно установить сервис Ядра LogAnalyzer с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

- Расширить кластер и добавить необходимое количество сервисов Ядра LogAnalyzer 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 LogAnalyzer.

  После запуска установщика expand.sh с подготовленным файлом инвентаря expand.inventory.yml никакие дополнительные сервисы Ядра LogAnalyzer 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 LogAnalyzer на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра LogAnalyzer в веб-интерфейсе и последовательно установить сервис Ядра LogAnalyzer с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

- Обновить распределенную установку LogAnalyzer 3.4 до распределенной установки с Ядром LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer на сервере указанном в группе kuma_core. После завершения работы установщика вам необходимо вручную создать сервисы Ядра LogAnalyzer в веб-интерфейсе и последовательно установить сервис Ядра LogAnalyzer с уникальным идентификатором на каждом сервере, указанном в группе kuma_core_peers.

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

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

Подготовка контрольной машины

Чтобы подготовить контрольную машину для установки LogAnalyzer:

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

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 LogAnalyzer.

Подготовка целевой машины

Чтобы подготовить целевую машину для установки компонентов LogAnalyzer:

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 LogAnalyzer после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами программы.
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 LogAnalyzer.
4. Чтобы получить имя хоста, которое потребуется указать при установке LogAnalyzer, 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 LogAnalyzer.

Подготовка файла инвентаря distributed.inventory.yml для установки LogAnalyzer с несколькими сервисами Ядра LogAnalyzer в кластере Raft

Установка, обновление и удаление компонентов LogAnalyzer производится из папки с распакованным установщиком с помощью инструмента Ansible® и созданного пользователем *файла инвентаря* в формате YML с перечнем хостов компонентов LogAnalyzer и других параметров.

Чтобы создать файл инвентаря distributed.inventory.yml для установки LogAnalyzer с несколькими сервисами Ядра LogAnalyzer в кластере Raft:

1. Перейдите в директорию установщика LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer.

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

Пример файла инвентаря distributed.inventory.yml для установки LogAnalyzer с несколькими сервисами Ядра LogAnalyzer 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 LogAnalyzer в кластере Raft

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

Чтобы установить LogAnalyzer:

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

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

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

   - Если вы планируете использовать активацию приложения 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 приложения с помощью лицензионного кода, 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 distributed.inventory.yml
   ```

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

   ```
   sudo ./install.sh single.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 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
          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.

  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:
      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
          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, программа не будет установлена.

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

   - Если вы планируете использовать активацию программы 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 LogAnalyzer на сервере из секции `kuma_core`, установлены дополнительные Ядра LogAnalyzer на серверах из секции `kuma_core_peers`, установлены все заданные в файле инвентаря сервисы и OOTB-ресурсы.

   - Если вы планируете использовать активацию приложения с помощью лицензионного кода, или планируете предоставить файл ключа позднее, в результате запуска установщика с файлом инвентаря distributed.inventory.yml будет установлено только Ядро LogAnalyzer на сервере из секции `kuma_core` и дополнительные Ядра LogAnalyzer на серверах из секции `kuma_core_peers`.

     Чтобы установить сервисы, в консоли командной строки укажите лицензионный код. 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 LogAnalyzer и в строке браузера введите адрес веб-интерфейса LogAnalyzer, а затем на странице входа введите учетные данные.

   Адрес веб-интерфейса LogAnalyzer – `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 LogAnalyzer установлены и выполнен вход в веб-интерфейс.

При дальнейшей установке сервисов LogAnalyzer вы можете указать в команде установки несколько URL через запятую для подключения к сервисам Ядра LogAnalyzer в кластере Raft.

Если в кластере Raft вы не используете балансировщик, вы можете входить на узел с Ядром LogAnalyzer напрямую. Если вы переходите с узла на узел, сессия, открытая на предыдущем узле, будет закрыта в момент успешной аутентификации на следующем узле.

Если вы хотите использовать доменную аутентификацию через AD FS, чтобы на каждом узле не требовалась отдельная аутентификация, вам необходимо настроить в кластере Raft балансировщик, в параметрах настройки AD FS указать FQDN балансировщика и затем настроить в LogAnalyzer доменную аутентификацию через AD FS, указав в параметрах FQDN балансировщика.

Все серверы, на которых развернуты сервисы Ядра LogAnalyzer должны быть в одном часовом поясе.

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

Расширение кластера Raft

Расширение кластера Raft в LogAnalyzer состоит из следующих этапов:

1. Подготовка серверов к установке сервисов Ядра LogAnalyzer.

   Установщик expand.sh, который вы запускаете на контрольной машине, готовит на целевых машинах необходимые файлы для последующей установки дополнительных сервисов Ядра LogAnalyzer.

2. Создание и установка дополнительных сервисов Ядра LogAnalyzer.

   Вам нужно будет создать дополнительные сервисы Ядра LogAnalyzer в веб-интерфейсе и последовательно установить сервис Ядра LogAnalyzer на серверах, указанных в группе kuma_core_peers в файле инвентаря expand.inventory.yml.

3. Актуализация файла инвентаря distributed.inventory.yml.

   Следует актуализировать данные в файле инвентаря distributed.inventory.yml на случай обновления LogAnalyzer.

Подготовка серверов к установке сервисов Ядра LogAnalyzer

Чтобы подготовить серверы к последующей установке дополнительных сервисов Ядра LogAnalyzer:

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

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

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

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

3. 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 LogAnalyzer

   ```
   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
   ```

4. На контрольной машине с доступом root из папки с распакованным установщиком выполните следующую команду:

   ./expand.sh expand.inventory.yml

5. Примите условия Лицензионного соглашения.

   Если вы не примете условия Лицензионного соглашения, программа не будет установлена.

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

   - Если вы планируете использовать активацию приложения 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 LogAnalyzer.

   - Если вы планируете использовать активацию приложения с помощью лицензионного кода, или планируете предоставить файл ключа позднее, в результате запуска установщика с файлом инвентаря expand.inventory.yml будет установлено только Ядро LogAnalyzer.

В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря expand.inventory.yml, появятся файлы для создания и установки дополнительных сервисов Ядра LogAnalyzer.

Создание и установка дополнительных сервисов Ядра LogAnalyzer

Поскольку сервисы Ядра LogAnalyzer состоят из двух частей, клиентской и серверной, вы будете создавать сервисы в два этапа:

1. Создание клиентской части сервиса Ядра LogAnalyzer 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 LogAnalyzer и на панели инструментов нажмите ⋮, в открывшемся меню нажмите **Копировать идентификатор**. Идентификатор сервиса Ядра LogAnalyzer понадобится для установки сервиса на сервере.

2. Создание серверной части сервиса Ядра LogAnalyzer.

   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 LogAnalyzer>:7210 --id <идентификатор сервиса Ядра LogAnalyzer, скопированный в веб-интерфейсе> --install
   ```

Повторите создание клиентской и серверной части сервиса Ядра LogAnalyzer для каждого хоста из группы kuma_core_peers. На каждом хосте может быть установлен только один сервис Ядра LogAnalyzer.

Актуализация файла инвентаря distributed.inventory.yml

Впишите группу kuma_core_peers в файле инвентаря distributed.inventory.yml и укажите серверы для дополнительных сервисов Ядра LogAnalyzer, которые вы указывали в файле инвентаря expand.inventroy.yml, чтобы в файле инвентаря distributed.inventory.yml были актуальные сведения на случай обновления LogAnalyzer.

Расширение кластера завершено. Сервисы Ядра LogAnalyzer добавлены в кластер Raft и подключены к core-1. При установке остальных сервисов LogAnalyzer вы можете указать в команде установки несколько URL через запятую для подключения к сервисам Ядра LogAnalyzer в кластере Raft.

Поддерживаемые сценарии установки и обновления с 3.4.x до 4.x с установкой Ядра в кластере Raft

Поддерживаемые сценарии установки LogAnalyzer

Вариант установки 3.4.x	Вариант установки 4.x.x	Поддержка и реализация
–	Установка на одном сервере или распределенная установка с одним сервисом Ядра LogAnalyzer	Выполняется установщиком автоматически. Используется файл инвентаря, аналогичный файлу инвентаря 3.4.x. Сервис Ядра LogAnalyzer на хосте, указанном в секции `kuma_core` имеет имя core-1 и идентификатор 00000000-0000-0000-0000-000000000000.
–	Установка на одном сервере с Ядром LogAnalyzer в кластере Raft или распределенная установка с Ядром LogAnalyzer в кластере Raft	Выполняется установщиком автоматически. Установщик готовит хосты из дополнительной секции `kuma_core_peers`, автоматически создает дополнительные сервисы Ядра LogAnalyzer и включает их в кластер Raft, устанавливая на хосты из этой секции. Сервис Ядра LogAnalyzer на хосте из секции `kuma_core` имеет имя core-1 и идентификатор 00000000-0000-0000-0000-000000000000. Сервисы Ядра LogAnalyzer на хостах из секции `kuma_core_peers` имеют имена вида core-<имя_хоста_в_файле_инвентаря> и уникальные идентификаторы.
Создание кластера Raft в установке 4.x.x с одним сервисом Ядра LogAnalyzer		Вы можете настроить дополнительные хосты с помощью установщика expand.sh и файла инвентаря expand.inventory.yml с заполненной секцией `kuma_core_peers`. После этого вам необходимо создать дополнительные сервисы Ядра LogAnalyzer в веб-интерфейсе LogAnalyzer и установить сервисы Ядра LogAnalyzer последовательно на подготовленных хостах с помощью команды установки.
Установка на одном сервере или распределенная установка	Установка на одном сервере с одним сервисом Ядра LogAnalyzer в кластере Raft или распределенная установка с одним сервисом Ядра LogAnalyzer в кластере Raft	Выполняется установщиком автоматически. Используется файл инвентаря, аналогичный версии 3.4.x. Имя и идентификатор сервиса Ядра LogAnalyzer на хосте из секции `kuma_core` не изменяются.
Установка на одном сервере или распределенная установка	Установка на одном сервере с несколькими сервисами Ядра LogAnalyzer в кластере Raft или распределенная установка с несколькими сервисами Ядра LogAnalyzer в кластере Raft	Сервисы Ядра LogAnalyzer должны размещаться каждый на отдельном хосте. Установщик только готовит хосты из дополнительной секции `kuma_core_peers` к последующей ручной установке дополнительных сервисов Ядра LogAnalyzer. После обновления до версии 4.x.x вам нужно создать дополнительные сервисы Ядра LogAnalyzer в веб-интерфейсе LogAnalyzer, которые автоматически будут добавлены в кластер. При необходимости вы можете настроить дополнительные хосты после обновления с помощью установщика expand.sh и файла инвентаря expand.inventory.yml, создать сервисы Ядра LogAnalyzer в веб-интерфейсе LogAnalyzer, установить сервисы Ядра LogAnalyzer на дополнительные хосты и включить сервисы в кластер. При обновлении для секций `kuma_core` и `kuma_core_peers` проводится проверка на уникальность хостов, аналогично установке с нуля. Если вы заполнили секцию `kuma_core_peers` при обновлении, для нее установщик install.sh выполняет действия, аналогичные отдельному запуску установщика expand.sh.
–	Установка с одним сервисом Ядра LogAnalyzer в кластере Kubernetes	Вы можете выполнить установку сервиса Ядра LogAnalyzer в одном экземпляре с двумя репликами тома. Вы можете использовать файл инвентаря, аналогичный версии 3.4.x. Для обеспечения отказоустойчивости требуется не менее двух рабочих узлов.
Установка с Ядром LogAnalyzer в кластере Kubernetes	Установка с одним сервисом Ядра LogAnalyzer в кластере Kubernetes	Сохраняется сервис Ядра LogAnalyzer в одном экземпляре с двумя репликами тома. Используется файл инвентаря, аналогичный файлу инвентаря 3.4.x. Поддержка нескольких сервисов Ядра LogAnalyzer в 4.x.x не предусмотрена.
Перенос установки 4.x.x с одним сервисом Ядра LogAnalyzer в установку с одним сервисом Ядра LogAnalyzer в кластере Kubernetes		Поведение аналогично миграции в установку в отказоустойчивой конфигурации для предыдущих версий LogAnalyzer. Вы можете установить сервис Ядра LogAnalyzer в одном экземпляре с двумя репликами тома. Используется файл инвентаря, аналогичный файлу инвентаря 3.4.x. Для обеспечения отказоустойчивости требуется не менее двух рабочих узлов. Хост, где был размещен сервис Ядра LogAnalyzer, становится одним из рабочих узлов кластера.

Резервное копирование LogAnalyzer

LogAnalyzer позволяет выполнять резервное копирование базы данных Ядра LogAnalyzer и сертификатов. Функция резервного копирования предназначена для восстановления LogAnalyzer. Для переноса или копирования ресурсов следует использовать функции экспорта и импорта ресурсов.

Резервное копирование можно выполнить с помощью REST API.

Вы также можете создавать резервные копии отдельных партиций с помощью процедуры архивирования.

Особенности резервного копирования LogAnalyzer

- Восстановление данных из резервной копии поддерживается только при сохранении версии LogAnalyzer.

  Если в LogAnalyzer 4.0 и выше выполнить резервное копирование, а затем восстановить резервную копию на другом устройстве с LogAnalyzer 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.

Изменение конфигурации LogAnalyzer

Доступны следующие изменения конфигурации LogAnalyzer.

- **Расширение установки "все в одном" до распределенной**.

Чтобы расширить установку "все в одном" до распределенной:

1. Создайте резервную копию LogAnalyzer.

2. Удалите с сервера предустановленные сервисы коррелятора, коллектора, хранилища и маршрутизатора событий.

   a. В веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** выберите сервис и нажмите **Копировать идентификатор**. На сервере, где были установлены сервисы, выполните команду удаления сервиса:

   ```
   sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage/eventRouter> --id
   <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --uninstall
   ```

   Повторите команду удаления для каждого сервиса.

   b. Затем удалите сервисы в веб-интерфейсе LogAnalyzer.

В результате на сервере первоначальной установки останется только Ядро LogAnalyzer.

3. Подготовьте файл инвентаря distributed.inventory.yml и укажите в нем сервер первоначальной установки "все в одном" в группе `kuma_core`.

   Таким образом Ядро LogAnalyzer останется на прежнем сервере, а остальные компоненты вы развернете на других серверах. Укажите серверы для установки компонентов LogAnalyzer в файле инвентаря.

   Пример файла инвентаря для расширения установки "все в одном" до распределенной

```
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
```

4. Создайте и установите сервисы хранилища, коллектора, коррелятора, маршрутизатора событий и агента на других машинах.

   a. После того, как вы заполните в файле инвентаря distributed.inventory.yml значения параметров для всех разделов, запустите установщик на контрольной машине.

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

   В результате выполнения команды на каждой целевой машине, указанной в файле инвентаря distributed.inventory.yml, появятся файлы, необходимые для установки компонентов LogAnalyzer: хранилища, коллекторов, корреляторов.

   b. Создайте сервисы хранилища, коллекторов и корреляторов.

Расширение установки завершено.

- **Добавление серверов для коллекторов в распределенную установку**.

В следующей инструкции показано, 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 установке.

2. На контрольной машине перейдите в директорию с распакованным установщиком LogAnalyzer, 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 укажите в нем серверы, которые вы хотите добавить, в разделе kuma_collector.

   Пример файла инвентаря expand.inventory.yml для добавления серверов для коллекторов

   ```
   kuma:
     vars:
       ansible_connection: ssh
       ansible_user: root
     children:
       kuma_collector:
         kuma-additional-collector1.example.com
         kuma-additional-collector2.example.com
       kuma_correlator:
       kuma_storage:
         hosts:
   ```

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 каждой целевой машине, указанной в файле инвентаря expand.inventory.yml, появятся файлы для создания и установки коллектора.

6. Создайте и установите коллекторы. Поскольку коллекторы LogAnalyzer состоят из двух частей, клиентской и серверной, вы будете создавать коллекторы в два этапа.

    1. Создание клиентской части коллектора, которая включает в себя набор ресурсов и сервис коллектора.

        Чтобы создать набор ресурсов для коллектора, в веб-интерфейсе LogAnalyzer 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, она отобразится на экране. Скопируйте команду установки и переходите к следующему шагу.

    2. Создание серверной части коллектора.

    a. 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 установлен на целевой машине. Вы можете проверить статус сервиса в веб-интерфейсе в разделе **Ресурсы** → **Активные сервисы**.

    b. Повторите выполнение команды 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 LogAnalyzer.

Добавление серверов завершено.

- Добавление серверов в существующий кластер хранения.

В следующей инструкции показано, как добавить несколько 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 установке.

2. На контрольной машине перейдите в директорию с распакованным установщиком LogAnalyzer, 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 укажите в нем серверы, которые вы хотите добавить, в разделе storage. В следующем примере в разделе 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 LogAnalyzer, последовательно выполняя шаги инструкции. Вы можете адаптировать этот пример 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:
           kuma-storage-cluster1-server9.example.com:
           kuma-storage-cluster1-server10.example.com:
           kuma-storage-cluster1-server11.example.com:
   ```

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 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 разделе **Ресурсы** → **Хранилища** выберите существующее хранилище и откройте его для редактирования.

   b. В разделе **Узлы кластера ClickHouse** нажмите **Добавить узлы** и в появившихся полях для нового узла укажите роли. В следующем 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:

      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. Чтобы создать сервис хранилища, в веб веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

   В открывшемся окне **Выберите сервис** выберите измененное на предыдущем шаге хранилище и нажмите **Создать сервис**. Повторите для каждого добавляемого узла хранилища ClickHouse.

   В результате количество созданных сервисов должно равняться количеству добавляемых узлов в кластере ClickHouse, то есть четыре узла - четыре сервиса. Созданные сервисы хранилища отображаются в веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы**.

8. Теперь сервисы хранилища необходимо установить на каждом сервере, используя идентификатор сервиса.

   a. В веб-интерфейсе LogAnalyzer **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.

   b. 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 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 разделе storage в файле инвентаря expand.inventory.yml. На каждой машине в команде установки следует указывать уникальный идентификатор сервиса в рамках кластера.

9. Чтобы применить изменения в работающем кластере, в веб-интерфейсе LogAnalyzer 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 LogAnalyzer.

Добавление серверов в кластер хранения завершено.

- Добавление дополнительного кластера хранения

В следующей инструкции показано, 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 установке.

2. На контрольной машине перейдите в директорию с распакованным установщиком LogAnalyzer, 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 укажите в нем серверы, которые вы хотите добавить, в разделе storage. В следующем примере в разделе storage указаны серверы для установки трех выделенных киперов и двух шардов, каждый из которых будет содержать по две реплики. В файле инвентаря expand.inventory.yml следует указать только FQDN, роли киперов, шардов и реплик вы будете назначать позднее в веб-интерфейсе LogAnalyzer, 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
           kuma-storage-cluster2-server2.example.com
           kuma-storage-cluster2-server3.example.com
           kuma-storage-cluster2-server4.example.com
           kuma-storage-cluster2-server5.example.com
           kuma-storage-cluster2-server6.example.com
           kuma-storage-cluster2-server7.example.com
   ```

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 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 три кластера хранения - три хранилища. Поскольку хранилище состоит из двух частей, клиентской и серверной, вы будете создавать хранилище в два этапа.

   1. Создание клиентской части хранилища, которая включает в себя набор ресурсов и сервис хранилища.

      a. Чтобы создать набор ресурсов для хранилища, в веб-интерфейсе LogAnalyzer 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.

      b. Чтобы создать сервис хранилища, в веб веб-интерфейсе LogAnalyzer 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.

      В результате количество созданных сервисов должно равняться количеству узлов в кластере ClickHouse, то есть пятьдесят узлов - пятьдесят сервисов. Созданные сервисы хранилища отображаются в веб-интерфейсе LogAnalyzer в разделе **Ресурсы → Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор сервиса.

   2. Создание серверной части хранилища.

   a. На целевой машине создайте серверную часть хранилища: в веб-интерфейсе LogAnalyzer **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.

   b. 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 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 разделе storage в файле инвентаря expand.inventory.yml. На каждой машине в команде установки следует указывать уникальный идентификатор сервиса в рамках кластера.

   d. 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 LogAnalyzer.

Добавление дополнительного кластера хранения завершено.

- **Удаление серверов из распределенной установки**.

Чтобы удалить сервер из распределенной установки:

1. Удалите все сервисы с сервера, который вы планируете удалить из распределенной установки.

   a. Удалите серверную часть сервиса. Скопируйте в веб-интерфейсе LogAnalyzer идентификатор сервиса и запустите на целевой машине следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma <collector/correlator/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> --uninstall
   ```

   b. Удалите клиентскую часть сервиса в веб-интерфейсе LogAnalyzer в разделе **Активные сервисы** – **Удалить**.

   Сервис удален.

2. Повторите шаг 1 для каждого сервера, который вы хотите удалить из инфраструктуры.

3. Удалите серверы из соответствующих разделов файла инвентаря distributed.inventory.yml, чтобы в файле инвентаря были актуальные сведения на случай обновления LogAnalyzer.

Серверы удалены из распределенной установки.

- Удаление кластера хранения из распределенной установки.

  Чтобы удалить один или несколько кластеров хранения из распределенной установки:

  1. Удалите сервис хранилища на каждом сервере кластера, подлежащем удалению из распределенной установки.

     a. Удалите серверную часть сервиса хранилища. Скопируйте в веб-интерфейсе LogAnalyzer идентификатор сервиса и запустите 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 LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** → **Удалить**.

     Сервис удален.

  2. Удалите серверы из раздела storage в файле инвентаря distributed.inventory.yml, чтобы в файле инвентаря были актуальные сведения на случай обновления LogAnalyzer или изменения конфигурации.

  Кластер удален из распределенной установки.

- Перенос Ядра LogAnalyzer в новый кластер Kubernetes.

Чтобы перенести Ядро LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer

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 LogAnalyzer в каталоге /usr/lib/systemd/system вручную, то при обновлении с предыдущей версии LogAnalyzer эти изменения будут потеряны. Если потребуется, внесите изменения повторно после обновления приложения.

Обновление с версии 2.0.x до 2.1.3

Чтобы установить LogAnalyzer версии 2.1.3 поверх версии 2.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить резервную копию для версии 2.0.

   Резервные копии LogAnalyzer, созданные в версии 2.0 и ниже, не подлежат восстановлению в версии 2.1.3. Это означает, что невозможно установить LogAnalyzer 2.1.3 и восстановить в ней резервную копию LogAnalyzer 2.0.

   Сразу после обновления LogAnalyzer до версии 2.1.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. Убедитесь в совместимости версий MongoDB, выполнив на устройстве с Ядром LogAnalyzer 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 LogAnalyzer с хостов хранилищ LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer.
   - 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 LogAnalyzer

1. В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

- 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 LogAnalyzer, 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 LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
   &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
    &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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, LogAnalyzer может все равно возвращать ошибку, потому что LogAnalyzer 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Создайте заново правила сегментации алертов.
3. Вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer успешно выполнено.

Обновление с версии 2.1.x до 2.1.3

Чтобы установить LogAnalyzer версии 2.1.3 поверх версии 2.1.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить резервную копию для версии 2.1.x.

   Резервные копии LogAnalyzer, созданные в версии ниже 2.1.3, не подлежат восстановлению в версии 2.1.3. Это означает, что невозможно установить LogAnalyzer 2.1.3 и восстановить в ней резервную копию LogAnalyzer 2.1.x.

   Сразу после обновления LogAnalyzer до версии 2.1.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре LogAnalyzer с хостов хранилищ LogAnalyzer.

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 LogAnalyzer

1. В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

   - Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

   - 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 LogAnalyzer, 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 LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
   &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
    &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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, LogAnalyzer может все равно возвращать ошибку, потому что LogAnalyzer 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer успешно выполнено.

Обновление с версии 2.1.3 до 3.0.3

Чтобы установить LogAnalyzer версии 3.0.3 поверх версии 2.1.3, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.3.

   Резервные копии LogAnalyzer, созданные в версии 2.1.3 и ниже, не подлежат восстановлению в версии 3.0.3. Это означает, что невозможно установить LogAnalyzer 3.0.3 и восстановить в ней резервную копию LogAnalyzer 2.1.3.

   Сразу после обновления LogAnalyzer до версии 3.0.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре LogAnalyzer с хостов хранилищ LogAnalyzer.

Обновление LogAnalyzer

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

- 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 LogAnalyzer, 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 LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer версии 3.0.3 поверх версии 3.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.x.

   Резервные копии LogAnalyzer, созданные в версии ниже 3.0.3, не подлежат восстановлению в версии 3.0.3. Это означает, что невозможно установить LogAnalyzer 3.0.3 и восстановить в ней резервную копию LogAnalyzer 3.0.x.

   Сразу после обновления LogAnalyzer до версии 3.0.3 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. На время установки или обновления обеспечьте сетевую доступность порта 7220 TCP на Ядре LogAnalyzer с хостов хранилищ LogAnalyzer.

Обновление LogAnalyzer

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

- 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 LogAnalyzer, 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 LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer 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 LogAnalyzer версии 3.2.x поверх версии 3.0.3, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить данные из резервной копии для версии 3.0.3.

   Резервные копии LogAnalyzer, созданные в версии 3.0.3 и ниже, не подлежат восстановлению в версии 3.2.x. Это означает, что невозможно установить LogAnalyzer 3.2.x и восстановить в ней резервную копию 3.0.3.

   Сразу после обновления LogAnalyzer до версии 3.2.x создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. Убедитесь, что имя хоста Ядра LogAnalyzer не начинается с цифры. Обновление до версии 3.2.x не может быть выполнено успешно, если имя хоста Ядра LogAnalyzer 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 LogAnalyzer с хостов хранилищ LogAnalyzer.

Обновление LogAnalyzer

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

- 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 LogAnalyzer, 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 LogAnalyzer в кластер Kubernetes уже выполнен и больше не требуется.

Чтобы перенести Ядро LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer. При необходимости вы сможете восстановить данные из резервной копии для версии 3.2.

   Резервные копии LogAnalyzer, созданные в версии 3.2 и ниже, не подлежат восстановлению в версии 3.4. Это означает, что невозможно установить LogAnalyzer 3.4 и восстановить в ней резервную копию 3.2.x.

   Сразу после обновления LogAnalyzer до версии 3.4 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. Убедитесь, что имя хоста Ядра LogAnalyzer не начинается с цифры. Обновление до версии 3.4 не может быть выполнено успешно, если имя хоста Ядра LogAnalyzer начинается с цифры. Если имя хоста Ядра LogAnalyzer 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 LogAnalyzer с хостов хранилищ LogAnalyzer.

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 LogAnalyzer для всех источников событий с красным статусом, для которых настроена отправка уведомлений о срабатывании политики, будут отправлены уведомления на указанные адреса электронной почты.

Обновление LogAnalyzer

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.
- 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 LogAnalyzer, 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 LogAnalyzer в кластер Kubernetes уже выполнен и больше не требуется.

Чтобы перенести Ядро LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/ &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты LogAnalyzer.

Обновление LogAnalyzer 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 LogAnalyzer версии 4.0 поверх версии 3.4.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра LogAnalyzer. При необходимости вы сможете восстановить данные из резервной копии для версии 3.4.x.

   Резервные копии LogAnalyzer, созданные в версии 3.4.x и ниже, не подлежат восстановлению в версии 4.0. Это означает, что невозможно установить LogAnalyzer 4.0 и восстановить в ней резервную копию 3.4.x.

   Сразу после обновления LogAnalyzer до версии 4.0 создайте резервную копию.

2. Убедитесь, что соблюдены все требования к установке программы.

3. Убедитесь, что имя хоста Ядра LogAnalyzer не начинается с цифры. Обновление до версии 4.0 не может быть выполнено успешно, если имя хоста Ядра LogAnalyzer начинается с цифры. Если имя хоста Ядра LogAnalyzer 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 LogAnalyzer с хостов хранилищ LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer в кластере Kubernetes запустите скрипт для определения размера данных метрик на томе Ядра LogAnalyzer 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 LogAnalyzer

В зависимости от используемой схемы развертывания KUMA выполните следующие действия:

- Используйте подготовленный файл инвентаря distributed.inventory.yml и следуйте инструкции по распределенной установке программы.

- Используйте подготовленный файл инвентаря k0s.inventory.yml и следуйте инструкции по распределенной установке в отказоустойчивой конфигурации с Ядром LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer в кластер Kubernetes уже выполнен и больше не требуется.

Чтобы перенести Ядро LogAnalyzer 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 программы. 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 LogAnalyzer в новый кластер Kubernetes

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

Устранение ошибки невозможности переноса Ядра LogAnalyzer

Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes может прерываться из-за превышения времени ожидания на шаге `Deploy Core transfer job`. После этого в журнале задач переноса core-transfer появится следующая запись об ошибке:

```
cp: can't stat '/mnt/kuma-source/core/.lic': No such file or directory
```

Чтобы предотвратить появление ошибки до начала переноса Ядра LogAnalyzer:

1. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.
2. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

3. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

   ```
   cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
   &&
   ```

4. Сохраните изменения в файле.

После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

Если вы начали перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes и он завершился с ошибкой, вам нужно выполнить шаги ниже, чтобы исправить ошибку.

Чтобы исправить ошибку после попытки переноса Ядра LogAnalyzer с хоста в новый кластер Kubernetes:

1. На любом контроллере кластера удалите объект Ingress, выполнив следующую команду:

   ```
   sudo k0s kubectl delete daemonset/ingress -n ingress
   ```

2. Проверьте, существует ли задача переноса в кластере:

   ```
   sudo k0s kubectl get jobs -n kuma
   ```

3. Если задача переноса существует, удалите ее:

   ```
   sudo k0s kubectl delete job core-transfer -n kuma
   ```

4. Перейдите в консоль хоста из группы kuma_core.
5. Запустите сервисы Ядра LogAnalyzer, выполнив следующие команды:

   ```
   sudo systemctl start kuma-mongodb
   sudo systemctl start kuma-core-00000000-0000-0000-0000-000000000000
   ```

6. Убедитесь, что сервис kuma-core-00000000-0000-0000-0000-000000000000 запущен успешно:

   ```
   sudo systemctl status kuma-core-00000000-0000-0000-0000-000000000000
   ```

7. Убедитесь, что из группы kuma_core есть доступ в интерфейс KUMA по FQDN хоста.

   Другие хосты при этом могут быть остановлены.

8. Перейдите в папку с распакованным установщиком и откройте файл roles/k0s_prepare/templates/core-transfer-job.yaml.j2 для изменения.

9. В файле core-transfer-job.yaml.j2 найдите следующие строки:

   ```
   cp /mnt/kuma-source/core/.lic {{ core_k0s_home }}/ &&
   cp /mnt/kuma-source/core/.tenantsEPS {{ core_k0s_home }}/ &&
   ```

10. Измените эти строки следующим образом с сохранением отступов, задающихся пробелами:

    ```
    cp /mnt/kuma-source/core/{{ core_uid }}/.lic {{ core_k0s_home }}/ &&
    cp /mnt/kuma-source/core/{{ core_uid }}/.tenantsEPS {{ core_k0s_home }}/
    &&
    ```

11. Сохраните изменения в файле.

    После этого вы можете повторно запустить распределенную установку с использованием подготовленного файла инвентаря k0s.inventory.yaml. Перенос Ядра LogAnalyzer с хоста в новый кластер Kubernetes будет выполнен успешно.

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

Для коллекторов 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-mongodb, kuma-victoria-metrics, kuma-vmalert, kuma-grafana.
- 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 LogAnalyzer в распределенной установке до последней версии LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer на сервере указанном в группе `kuma_core`. После завершения работы установщика вам необходимо вручную создать сервисы Ядра LogAnalyzer в веб-интерфейсе и последовательно установить сервис Ядра LogAnalyzer с уникальным идентификатором на каждом сервере, указанном в группе `kuma_core_peers`.

  После обновления все существующие сервисы LogAnalyzer будут подключены к Ядру LogAnalyzer 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 LogAnalyzer в кластере Raft.

Финальный этап подготовки LogAnalyzer к работе

1. После обновления LogAnalyzer очистите кеш браузера.
2. Если вы используете агенты, вручную обновите агенты LogAnalyzer.
3. Выполните миграцию событий алертов из MongoDB в ClickHouse.
4. Укажите хранилище для новых событий алертов в параметрах наполнения алертов.

Обновление LogAnalyzer 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.

Устранение ошибок при обновлении

При обновлении LogAnalyzer вы можете столкнуться со следующими ошибками:

- **Ошибка по таймауту**

  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, LogAnalyzer может все равно возвращать ошибку, потому что из-за предельных ресурсов и ошибки по таймауту LogAnalyzer не удалось запустить сервис Ядра. Если вы введете пароль администратора трижды, не дожидаясь завершения установки, обновление может завершиться фатальной ошибкой.

  Выполните следующие шаги, чтобы устранить ошибку по таймауту и успешно завершить обновление:

  1. Откройте отдельный второй терминал и запустите следующую команду, чтобы убедиться, что вывод команды содержит строку с сообщением об ошибке таймауту:

     ```
     journalctl -u kuma-core | grep 'start operation timed out'
     ```

     Сообщение об ошибке по таймауту:

     kuma-core.service: start operation timed out. Terminating.

  2. После того, как вы нашли сообщение об ошибке по таймауту, 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.

     LogAnalyzer 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 настройки 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 настройки 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 LogAnalyzer хранилище может быть в красном статусе, а в его журналах могут отображаться ошибки о подозрительных строках.

  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 LogAnalyzer:

  ```
  touch /opt/kaspersky/kuma/clickhouse/data/flags/force_restore_data && systemctl
  restart kuma-storage-<идентификатор_хранилища,_в_котором_обнаружена_ошибка>
  ```

- **Истечение срока действия сертификатов кластера k0s**

Симптомы

Невозможно подключение контроллеров или рабочих узлов, перенос подов 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 - 1 год. Используемый в отказоустойчивой установке LogAnalyzer 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 - сертификаты будут перевыпущены:

```
systemctl restart k0scontroller
```

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.

Устраните ошибки, чтобы успешно завершить обновление.

Удаление LogAnalyzer

При удалении LogAnalyzer используется инструмент Ansible и созданный пользователем файл инвентаря.

Чтобы удалить LogAnalyzer:

1. На контрольной машине войдите в директорию установщика:

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

2. Выполните следующую команду:

   ```
   sudo ./uninstall.sh <файл инвентаря>
   ```

LogAnalyzer и все данные программы удалены с серверов.

Базы данных, которые использовались LogAnalyzer (например, база данных хранилища ClickHouse), и содержащуюся в них информацию следует удалить отдельно.

Особенности удаления LogAnalyzer, установленной в отказоустойчивом варианте

Состав удаляемых компонентов зависит от значения параметра `deploy_to_k8s` в файле инвентаря, используемого для удаления LogAnalyzer:

- `true` – удаляется созданный при установке LogAnalyzer кластер Kubernetes.
- `false` – из кластера Kubernetes удаляются все компоненты LogAnalyzer, кроме Ядра. Сам кластер не удаляется.

Помимо установленных вне кластера компонентов LogAnalyzer 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 LogAnalyzer с тем же файлом инвентаря.

После удаления LogAnalyzer необходимо перезагрузить хосты, на которых были установлены компоненты LogAnalyzer 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 LogAnalyzer **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 LogAnalyzer **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 LogAnalyzer 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 LogAnalyzer **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.

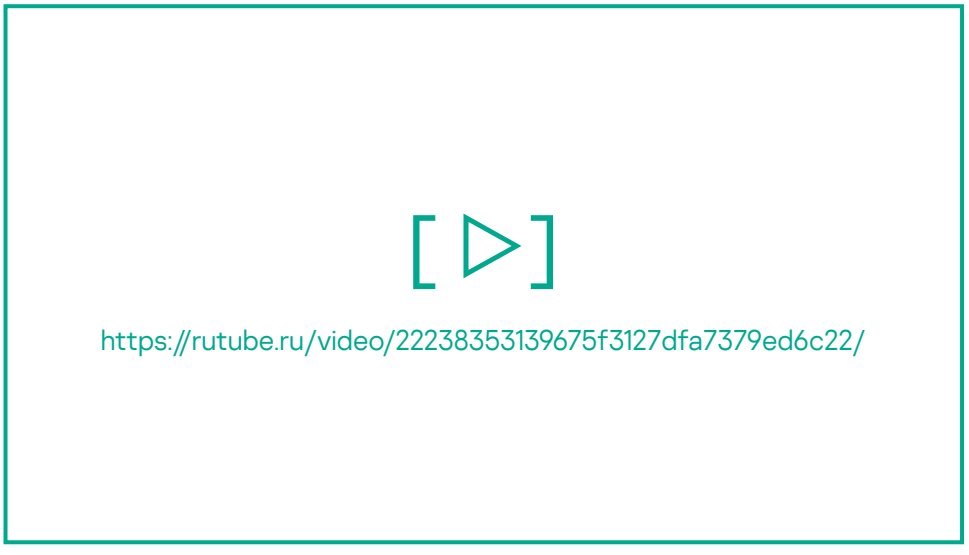
3. Нажмите **OK**.

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 LogAnalyzer можно выбрать, данные каких тенантов будут отображаться в веб-интерфейсе LogAnalyzer.

Чтобы выбрать тенант для отображения данных:

1. В веб-интерфейсе LogAnalyzer нажмите **Выбрано тенантов**.

   Откроется область выбора тенантов.

2. Установите флажки напротив тенантов, данные которых вы хотите видеть в разделах веб-интерфейса LogAnalyzer.

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 LogAnalyzer 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, панелей мониторинга, шаблонов отчетов, виджетов и других параметров LogAnalyzer, где можно выбрать тенант.

Правила принадлежности к тенантам

Важно отслеживать, какому тенанту принадлежат создаваемые в LogAnalyzer объекты: от этого зависит, кто к ним будет иметь доступ и взаимодействие с какими объектами можно настроить.

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.

> Сервисы, которые должны быть размещены на мощностях главного тенанта, разворачиваются только пользователями с ролью главный администратор.

Управление пользователями

Доступ к LogAnalyzer 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 LogAnalyzer **Параметры** → **Пользователи**. Пользователи также создаются в программе автоматически, если включена интеграция LogAnalyzer с Active directory и пользователь входит в веб-интерфейс LogAnalyzer с помощью своей доменной учетной записи в первый раз.

Всем внутренним пользователям, чьи учетные записи были созданы в веб-интерфейсе LogAnalyzer, кроме учетной записи admin, нужно сменить пароль при первом входе в веб-интерфейс LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer **Параметры** → **Доступы** → **Пользователи** → **Активные пользователи** установите флажок напротив нужного пользователя и нажмите **Выключить**.

Роли пользователей

Функциональные возможности, связанные с интеграцией Kaspersky CyberTrace и Kaspersky Threat Lookup, доступны только в коммерческой версии LogAnalyzer.

Пользователи LogAnalyzer могут иметь следующие роли:

- *Главный администратор* – эта роль предназначена для пользователей, отвечающих за функционирование основных систем LogAnalyzer. Например, они устанавливают системные компоненты, выполняют обслуживание, работают с сервисами, создают резервные копии и добавляют пользователей в систему. Эти пользователи имеют полный доступ к LogAnalyzer.
- *Администратор тенанта* – эта роль предназначена для пользователей, отвечающих за функционирование систем LogAnalyzer, принадлежащих определенным тенантам.
- *Аналитик второго уровня* – эта роль предназначена для пользователей, ответственных за настройку системы LogAnalyzer для получения и обработки событий определенного тенанта.
- *Аналитик первого уровня* – эта роль предназначена для пользователей, ответственных за настройку системы LogAnalyzer для получения и обработки событий определенного тенанта. 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.

- *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 редактирование общих ресурсов.

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
Создавать шаблон отчета	есть	есть	есть	есть	нет	нет	нет
Просматривать и изменять шаблоны и отчеты	есть	есть	есть	есть	нет	нет	нет
Формировать отчеты	есть	есть	есть	есть	нет	нет	нет
Просматривать сформированные отчеты	есть	есть	есть	есть	есть	нет	нет
Изменять сформированные отчеты	есть	есть	есть	есть	нет	нет	нет
Выгружать сформированные отчеты	есть	есть	есть	есть	есть	нет	нет
Удалять шаблоны и сформированные отчеты	есть	есть	есть	есть	нет	нет	нет
Изменять параметры формирования отчетов	есть	есть	есть	только параметры своих отчетов	нет	нет	нет
Дублировать шаблон отчета	есть	есть	есть	есть	нет	нет	нет
Открывать сформированный отчет по почте	есть	есть	есть	есть	есть	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
Просматривать данные на панели мониторинга и менять панели мониторинга	есть	есть	есть	есть	есть	нет	нет
Просматривать универсальную панель мониторинга	есть	есть	есть	есть	есть	нет	нет
Добавлять панели мониторинга	есть	есть	есть	есть	нет	нет	нет
Изменять и переименовывать панели мониторинга	есть	есть	есть	есть	нет	нет	нет

Удалять панели мониторинга	есть	есть	есть	есть	нет	нет	нет
Включать и выключать режим ТВ	есть	есть	есть	есть	есть	нет	нет

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
Просматривать список активных сервисов	есть	есть	есть	есть	есть	нет	нет
Просматривать и удалять партиции в хранилище	есть	нет	нет	нет	нет	нет	нет
Скачивать журналы сервисов	есть	есть	есть	есть	есть	нет	нет
Копировать ID сервиса	есть	есть	есть	есть	есть	нет	нет
Обновить таблицу с активными сервисами	есть	есть	есть	есть	есть	нет	нет
Перейти к событиям	есть	есть	есть	есть	есть	нет	нет
Создавать набор ресурсов для сервисов	есть	есть	есть	нет	нет	нет	нет
Создавать сервис в разделе Ресурсы → Сервисы → Активные сервисы	есть	есть	нет	нет	нет	нет	нет
Удалять сервисы	есть	есть	нет	нет	нет	нет	нет
Просматривать сервисы в сером статусе	есть	нет	нет	нет	нет	нет	нет
Перезапускать сервисы	есть	есть	нет	нет	нет	нет	нет
Обновлять параметры сервисов	есть	есть	есть	нет	нет	нет	нет
Сбрасывать сертификаты	есть	есть	нет	нет	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
Просматривать список конфигураций ресурсов и сервисов	есть	есть	есть	есть	нет	есть	есть
Создавать конфигурацию сервиса	есть	есть	есть	есть	нет	нет	нет
Создавать конфигурацию ресурса	есть	есть	есть	есть	нет	есть	нет
Дублировать конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	нет
Изменять конфигурацию ресурса/сервиса	есть	есть	есть	только своего ресурса	нет	есть	нет

Удалять конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	нет
Импортировать конфигурацию ресурса/сервиса из файла	есть	есть	есть	нет	нет	есть	нет
Просматривать репозиторий, импортировать ресурсы из репозитория	есть	есть	есть	нет	нет	нет	нет
Экспортировать конфигурацию ресурса/сервиса	есть	есть	есть	есть	нет	есть	есть
Создать и редактировать конфигурацию ресурса в Общем тенанте	есть	нет	нет	нет	нет	есть	нет
Просматривать ресурс в Общем тенанте (в том числе привязать, экспортировать, дублировать)	есть	нет	нет	нет	нет	есть	есть

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
Просматривать источники событий	есть	есть	есть	есть	есть	нет	нет
Изменять источники событий	есть	есть	есть	нет	нет	нет	нет
Удалять источники событий	есть	есть	есть	нет	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
Просматривать политики мониторинга	есть	есть	есть	есть	есть	есть	есть
Создавать политики мониторинга	есть	есть	есть	нет	нет	есть	нет
Изменять политики мониторинга	есть	есть	есть	нет	нет	есть	нет
Удалять политики мониторинга	есть	есть	есть	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
Просматривать список событий	есть	есть	есть	есть	есть	нет	нет
Выполнять поиск событий	есть	есть	есть	есть	есть	нет	нет
Открывать детали событий	есть	есть	есть	есть	есть	нет	нет
Открывать статистику	есть	есть	есть	есть	есть	нет	нет

Выгружать события в TSV-файл	есть	есть	есть	есть	есть	нет	нет
Просмотр фильтров (поисковый запрос)	есть	есть	есть	есть	есть	есть	есть
Добавить (сохранить) фильтр	есть	есть	есть	есть	есть	есть	нет
Изменять и удалять чужие папки фильтров	есть	есть	нет	нет	нет	нет	нет
Удалять свои фильтры	есть	есть	есть	есть	есть	есть	нет
Удалять чужие фильтры	есть	есть	нет	нет	нет	нет	нет
Запускать ktl-обогащение (доступно только в коммерческой версии LogAnalyzer)	есть	есть	есть	есть	нет	нет	нет
Добавить индикатор в Internal TI CyberTrace (доступно только в коммерческой версии LogAnalyzer)	есть	есть	есть	есть	нет	нет	нет
Создавать пресеты	есть	есть	есть	есть	есть	есть	нет
Удалять пресеты	есть	есть	есть	есть	есть	есть	нет
Просматривать и использовать пресеты	есть	есть	есть	есть	есть	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
Просматривать список пользователей	есть	нет	нет	нет	нет	нет	нет
Добавлять пользователя	есть	нет	нет	нет	нет	нет	нет
Изменять пользователя	есть	нет	нет	нет	нет	нет	нет
Генерировать токен	есть	есть	есть	есть	есть	есть	есть
Изменять права доступа для токена	есть	есть	есть	есть	есть	есть	есть
Просматривать данные своего профиля	есть	есть	есть	есть	есть	есть	есть
Изменять данные своего профиля	есть	есть	есть	есть	есть	есть	есть

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
Просматривать список тенантов	есть	нет	нет	нет	нет	нет	нет
Добавлять тенантов	есть	нет	нет	нет	нет	нет	нет
Изменять тенантов	есть	нет	нет	нет	нет	нет	нет
Экспортировать тенантов	есть	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
Просматривать параметры подключения к Active directory	есть	нет	нет	нет	нет	нет	нет
Изменять параметры подключения к Active directory	есть	нет	нет	нет	нет	нет	нет
Добавлять фильтры по ролям для тенантов	есть	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
Просматривать параметры подключения к SMTP	есть	нет	нет	нет	нет	нет	нет
Изменять параметры подключения к SMTP	есть	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
Просматривать список добавленных лицензионных ключей	есть	нет	нет	нет	нет	нет	нет
Добавлять лицензионные ключи	есть	нет	нет	нет	нет	нет	нет
Удалять лицензионные ключи	есть	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Kaspersky CyberTrace (доступно только в коммерческой версии LogAnalyzer)

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
Просматривать параметры интеграции с CyberTrace	есть	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с CyberTrace	есть	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

Права пользователей раздела Kaspersky Threat Lookup (доступно только в коммерческой версии LogAnalyzer)

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
Просматривать параметры интеграции с Threat Lookup	есть	нет	нет	нет	нет	нет	нет
Изменять параметры интеграции с Threat Lookup	есть	нет	нет	нет	нет	нет	нет

Раздел доступен только главному администратору.

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
Просматривать параметры	есть	есть	есть	нет	нет	нет	нет
Изменять параметры	есть	нет	нет	нет	нет	нет	нет
Запуск задачи обновление репозитория вручную	есть	есть	есть	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
Просмотр списка наборов	есть	нет	нет	нет	нет	нет	нет
Добавление, редактирование, удаление набора пространств	есть	нет	нет	нет	нет	нет	нет
Установка набора пространств по умолчанию	есть	нет	нет	нет	нет	нет	нет
Назначение пользователю набора пространств	есть	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
Просматривать список тегов	есть	есть	есть	есть	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
Открывать метрики	есть	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
Просматривать список своих задач	есть	есть	есть	есть	есть	нет	нет
Завершать свои задачи	есть	есть	есть	есть	есть	нет	нет
Перезапускать свои задачи	есть	есть	есть	есть	есть	нет	нет
Просматривать список всех задач	есть	есть	есть	есть	есть	нет	нет
Завершать любые задачи	есть	да	нет	нет	нет	нет	нет
Перезапускать любые задачи	есть	есть	есть	есть	есть	нет	нет

Права пользователей разделаCyberTrace (доступно только в коммерческой версии LogAnalyzer)

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
Открывать раздел	есть	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
Доступ к тенантам	есть	есть	есть	есть	есть	нет	нет
Общий тенант	есть	есть	есть	есть	есть	есть	есть
Главный тенант	есть	есть	есть	есть	есть	нет	нет

Настройка политики безопасности при входе в веб-интерфейс LogAnalyzer

Чтобы снизить риск несанкционированного доступа к веб-интерфейсу LogAnalyzer, вы можете настроить правила входа в веб-интерфейс LogAnalyzer для пользователей. Например, настроенная политика безопасности помогает предотвратить вход злоумышленника в веб-интерфейс LogAnalyzer с помощью перебора пароля.

Политика безопасности действует только на учетные записи пользователей, созданные в LogAnalyzer, и не действует на доменные учетные записи, импортированные в LogAnalyzer при интеграции с контроллерами доменов. При этом политика безопасности ограниченно действует на учетную запись admin, которая используется для первого входа в веб-интерфейс LogAnalyzer. 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 LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer:

1. Откройте раздел веб-интерфейса LogAnalyzer **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 LogAnalyzer с помощью автоматического перебора пароля. Укажите число от 1 до 8. Значение по умолчанию – 3. Если LogAnalyzer фиксирует превышение заданного значения, дальнейшие попытки аутентификации блокируются.

     Обратите внимание, что параметр указывается в расчете на одно Ядро LogAnalyzer. Если в вашем экземпляре LogAnalyzer развернуто больше одного Ядра LogAnalyzer, фактическое разрешенное количество попыток аутентификации в секунду будет равно указанному вами значению, умноженному на количество Ядер LogAnalyzer.

   - **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 LogAnalyzer. 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 приложения после истечения срока, указанного в параметре **Время жизни пароля (дни)**.

     Если этот параметр включен, попытка пользователя войти в веб-интерфейс LogAnalyzer будет заблокирована. Статус учетной записи пользователя сменится на *Неактивная*. Пользователь с таким статусом не может войти в веб-интерфейс LogAnalyzer. 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 LogAnalyzer. После этого LogAnalyzer автоматически предложит пользователю сменить пароль.

   - **Повторная аутентификация требуется после того, как пользователь неактивен в течение (мин)** – если во время сеанса в веб-интерфейсе LogAnalyzer не будет зафиксировано движение мыши или нажатия клавиш со стороны пользователя в течение указанного вами периода, LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 пользователя

Чтобы создать учетную запись пользователя:

1. Откройте раздел веб-интерфейса LogAnalyzer **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 LogAnalyzer 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 приложения 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.

   - **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от LogAnalyzer.

   - **Уведомлять об алертах в веб-интерфейсе** – установите этот флажок, чтобы в веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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, 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, 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 LogAnalyzer 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 LogAnalyzer пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс LogAnalyzer 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 нового пользователя. Пользователю можно назначить временный пароль и установить этот флажок. После входа с временным паролем LogAnalyzer 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 будет исполнять пользователь. 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 миграции 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 LogAnalyzer **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.

     В веб-интерфейс LogAnalyzer 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 приложения 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..

   - **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от LogAnalyzer.

   - **Уведомлять об алертах в веб-интерфейсе** – установите этот флажок, чтобы в веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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, 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, 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 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 LogAnalyzer пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс LogAnalyzer 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, LogAnalyzer будет отображать это пространство как `удалено+UUID` даже после сохранения изменений в наборе пространств.

Сервисы LogAnalyzer

Сервисы – это основные компоненты LogAnalyzer, с помощью которых система осуществляет работу с событиями: сервисы позволяют получить события из источников, чтобы в дальнейшем привести их к общему виду, удобному для хранения и ручного анализа. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри веб-интерфейса LogAnalyzer на основе набора ресурсов для сервисов.
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система LogAnalyzer, 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 LogAnalyzer располагаются в директории `/opt/kaspersky/kuma`.

  При установке LogAnalyzer в отказоустойчивом варианте в кластере устанавливается только Ядро LogAnalyzer. Коллекторы и хранилища размещаются на хостах вне кластера Kubernetes.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Типы сервисов:

- Хранилища – используются для хранения событий.
- Коллекторы – используются для получения события и конвертации их в формат LogAnalyzer.

- Агенты – используются для получения событий на удаленных устройствах и пересылки их в коллекторы LogAnalyzer.

- Маршрутизаторы событий – используются для приема потоков событий от коллекторов и дальнейшего распределения событий по заданным точкам назначения в соответствии с настроенными фильтрами.

В веб-интерфейсе LogAnalyzer 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**, **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 LogAnalyzer или какой-либо из выбранных сервисов находится в сером статусе. Чтобы кнопка **Обновить параметры** стала доступна для групповых действий, снимите флажок с сервиса Ядра LogAnalyzer 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 LogAnalyzer **Ресурсы** → **Активные сервисы**.

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса – расположенных внутри LogAnalyzer и установленных в сетевой инфраструктуре – в единый комплекс. Идентификатор присваивается сервису при его создании в LogAnalyzer, а затем используется при установке сервиса на сервер.

Чтобы получить идентификатор сервиса:

1. Войдите в веб-интерфейс LogAnalyzer и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом, идентификатор которого вы хотите получить, и нажмите **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 LogAnalyzer 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 LogAnalyzer.

Команды остановки, запуска и проверки статуса сервиса

Сервис	Остановить сервис	Запустить сервис	Проверить статус сервиса
Ядро	`sudo systemctl stop kuma-core-< идентификатор сервиса >.service`	`sudo systemctl start kuma-core-< идентификатор сервиса >.service`	`sudo systemctl status kuma-core-< идентификатор сервиса >.service`
Сервисы с идентификатором: • коллектор • хранилище	`sudo systemctl stop kuma-<collector/storage>-< идентификатор сервиса >.service`	`sudo systemctl start kuma-<collector/storage>-< идентификатор сервиса >.service`	`sudo systemctl status kuma-<collector/storage>-< идентификатор сервиса >.service`
Сервисы без идентификатора: • kuma-grafana.service • kuma-mongodb.service • kuma-victoria-metrics.service • kuma-vmalert.service	`sudo systemctl stop <grafana/victoria-metrics/vmalert>.service`	`sudo systemctl start <grafana/victoria-metrics/vmalert>.service`	`sudo systemctl status <grafana/victoria-metrics/vmalert>.service`
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 учётной 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 учётной записи с правами администратора. 4. Выполните в PowerShell команду: `Start-Service -Name "WindowsAgent-< идентификатор агента >"`	Чтобы просмотреть статус сервиса агента: 1. В ОС Windows перейдите в меню Start → Services и в списке сервисов откройте двойным щелчком нужный агент KUMA. 2. В открывшемся окне на вкладке General просмотрите статус агента в поле Service status.

Перезапуск сервиса

Чтобы перезапустить сервис:

1. Войдите в веб-интерфейс LogAnalyzer и откройте раздел **Ресурсы** → **Активные сервисы**.

2. Установите флажок рядом с сервисом и выберите нужную опцию:

   - **Обновить параметры** – обновить конфигурацию работающего сервиса, не останавливая его. Например, так можно изменить настройки сопоставления полей или параметры точки назначения.

   - **Перезапустить** – остановить сервис и запустить его снова. Эта опция используется для изменения таких параметров, как порт или тип коннектора.

     Особенности перезапуска агентов LogAnalyzer:

     - Агент LogAnalyzer 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 LogAnalyzer вы получите сообщение об ошибке. В этом случае следует перезапустить сервис Агент LogAnalyzer 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 LogAnalyzer 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. Эту опцию недопустимо использовать для обновления сертификата Ядра. Чтобы обновить сертификаты Ядра LogAnalyzer, их следует перевыпустить.

     Особенности удаления сертификатов для агентов Windows:

     - Если агент находится в зеленом статусе и вы выбрали **Сбросить сертификат**, LogAnalyzer удаляет действующий сертификат и создает новый, агент продолжает работу с новым сертификатом.

     - Если агент находится в красном статусе и вы выбрали **Сбросить сертификат**, LogAnalyzer выдаст 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 применить опцию **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 опция **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 LogAnalyzer:

1. Войдите в веб-интерфейс LogAnalyzer и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным сервисом и нажмите **Удалить**.

   Откроется окно подтверждения.
3. Нажмите **OK**.

Сервис удален из LogAnalyzer.

Чтобы удалить сервис с сервера, выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage/eventRouter/metrics> --id
< идентификатор сервиса > --uninstall
Сервис удален с сервера.
```

Окно Разделы

Создав и установив сервис хранилища, вы можете просмотреть его разделы в таблице **Разделы**.

*Чтобы открыть таблицу **Разделы**:*

1. Войдите в веб-интерфейс LogAnalyzer и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем и нажмите **Смотреть разделы**.

Откроется таблица **Разделы**.

В таблице есть следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные.
- **Создан** – дата создания раздела.
- **Пространство** – название раздела.
- **Размер** – размер раздела.
- **События** – количество хранимых событий.

- **Переход к холодному хранению** – дата, когда данные будут перенесены с кластеров ClickHouse на диски для холодного хранения.
- **Окончание хранения** – дата, когда истекает срок действия раздела. По достижении этого срока раздел и содержащиеся в нем события перестают быть доступны.

Вы можете удалять разделы.

Чтобы удалить раздел:

1. Откройте таблицу **Разделы** (см. выше).
2. Откройте раскрывающийся список ... слева от необходимого раздела.
3. Выберите **Удалить**.

   Откроется окно подтверждения.
4. Нажмите **OK**.

Раздел удален. Разделы для событий аудита удалить невозможно.

Поиск связанных событий

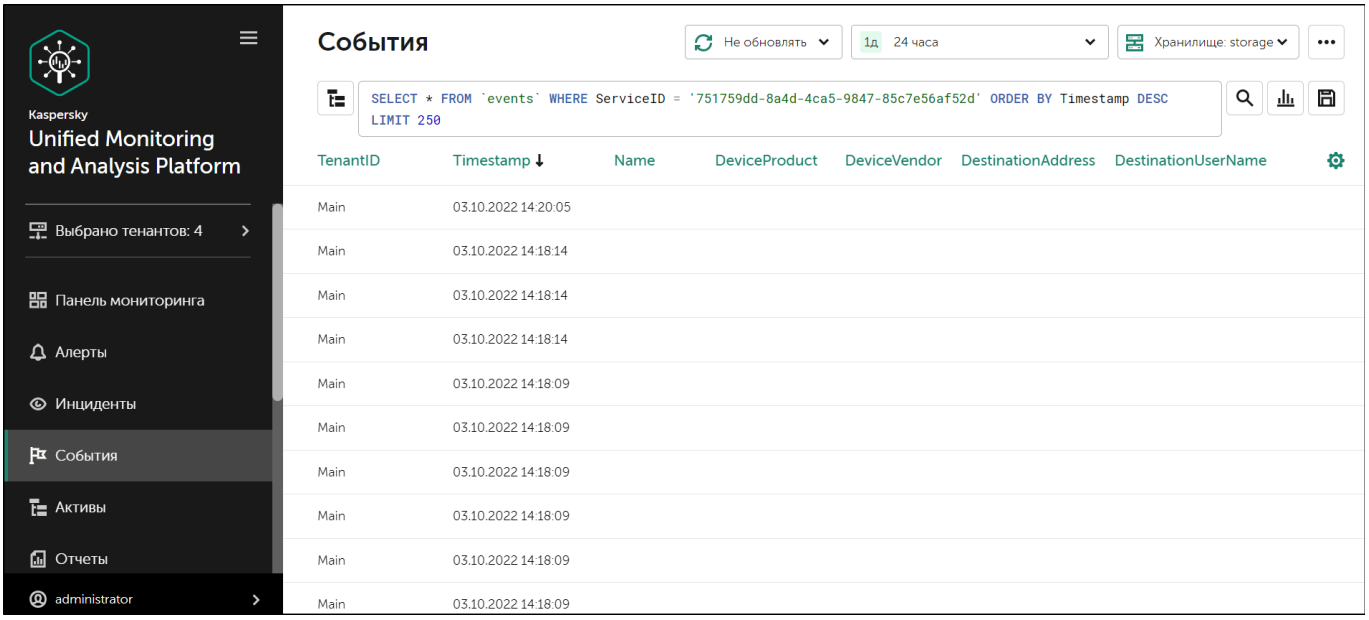
Вы можете искать события, обработанные определенным коллектором.

Чтобы найти события, относящиеся к коллектору:

1. Войдите в веб-интерфейс LogAnalyzer и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным коллектором и нажмите **Перейти к событиям**.

   Откроется новая вкладка браузера с открытым разделом LogAnalyzer **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 LogAnalyzer 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 коллектором.

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент LogAnalyzer, представляющий собой комплект настроек, на основе которых создаются и функционируют сервисы LogAnalyzer. 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 LogAnalyzer **Ресурсы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы
- 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 LogAnalyzer, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища LogAnalyzer 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 LogAnalyzer**
2. **Создание сервиса хранилища в веб-интерфейсе LogAnalyzer**
3. **Установка узлов хранилища в сетевой инфраструктуре**

При создании узлов кластера хранилища убедитесь в сетевой связности системы и откройте используемые компонентами порты.

При изменении параметров хранилища его сервис необходимо перезапустить.

Структура кластера ClickHouse

Кластер ClickHouse – логическая группа устройств, обладающих всеми накопленными нормализованными событиями LogAnalyzer. 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 LogAnalyzer, а также в координации репликации данных на уровне всего кластера.
- шард, реплика – узел участвует в накоплении и поиске нормализованных событий LogAnalyzer.
- 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 LogAnalyzer можно настроить перенос устаревших данных с кластера ClickHouse на холодное хранение. Для холодного хранения могут использоваться смонтированные в операционной системе локальные диски или распределенная файловая система Hadoop Distributed File System (HDFS). 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 по пути, указанному в конфигурации хранилища. Если диск холодного хранения не настроен и на сервере в горячем хранилище закончилось место, сервис хранилища остановится. Если есть горячее и холодное хранение и на диске холодного хранения закончилось место, сервис хранилища KUMA остановится. Мы рекомендуем избегать таких ситуаций с помощью добавления пользовательских условий хранения событий в горячем хранилище.

Диски холодного хранения можно добавлять и удалять. Если вы добавили несколько дисков холодного хранения, данные будут записываться на них по стандартному принципу чередования (англ. round-robin) по круговому циклу. Если данные, которые необходимо записать на диск, занимают больше места, чем свободно на этом диске, эти данные и все последующие будут записываться по принципу чередования на следующие диски холодного хранения. Если вы добавили только два диска холодного хранения, данные будут записываться на тот диск, на котором есть свободное место.

После изменения параметров холодного хранения сервис хранилища необходимо перезапустить. Если сервис не запускается, причина будет указана в журнале хранилища.

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 HDFS-дисков), 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. LogAnalyzer получает партиции для проверяемого хранилища и группирует их по дискам холодного хранения и пространствам.

2. Для каждого пространства LogAnalyzer 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), LogAnalyzer 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 LogAnalyzer создает события аудита.

4. Если настроен срок хранения данных в LogAnalyzer, 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 LogAnalyzer, решение удаляет эти события или все партиции за самую старую дату.

   При удалении данных LogAnalyzer создает события аудита.

Если диски кластера ClickHouse заполнены на 95%, самые большие партиции автоматически переносятся на диски холодного хранения. Это действие может происходить больше одного раза в час.

Во время переноса данных сервис хранилища продолжает работать, при этом в разделе веб-интерфейса LogAnalyzer **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 LogAnalyzer. Например, при поиске событий.
- 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:

- В веб-интерфейсе LogAnalyzer перейдите в раздел **Ресурсы** → **Хранилища** и выберите нужное хранилище.

  Откроется хранилище.

- В окне в разделе **Диски холодного хранения** в блоке параметров нужного диска нажмите **Удалить диск**.

  Данные с удаляемого диска автоматически начинают переноситься на другие диски холодного хранения или, если их нет, в кластер ClickHouse. В процессе переноса данных значок статуса хранилища светится желтым цветом и отображается значок песочных часов. При начале 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 DROP PARTITION.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо создать диск с таким же путем (для локальных дисков) или таким же адресом (для HDFS-дисков), а затем удалить его из параметров хранилища.

Отключение, архивирование и подключение партиций

Если вы хотите оптимизировать дисковое пространство и ускорить выполнение запросов в LogAnalyzer, 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, выполните следующие шаги:

1. Определите шард, на всех репликах которого вы планируете отключить партицию.

2. Получите идентификатор партиции с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/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 требуемый 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>'"
   ```

В результате партиция отключена на всех репликах шарда. Теперь вы можете перенести каталог с данными на носитель или заархивировать партицию.

Архивирование партиций

Чтобы архивировать отключенные партиции:

1. Найдите отключенную партицию в дисковой подсистеме сервера:

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <идентификатор отключенной партиции>\*
   ```

2. Перейдите в каталог detached с отключенной партицией и, находясь в каталоге detached, выполните архивирование:

   ```
   sudo cd <путь к каталогу detached, содержащему отключенную партицию>
   ```

   ```
   sudo zip -9 -r detached.zip *
   ```

   Например:

   ```
   sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

   ```
   sudo zip -9 -r detached.zip *
   ```

Архивирование партиции выполнено.

Подключение партиций

Чтобы подключить архивные партиции к LogAnalyzer, необходимо выполнить следующие действия:

1. Увеличьте значение параметра **Срок хранения**.

   LogAnalyzer удаляет данные на основании даты, указанной в поле Timestamp - когда событие получено, и на основании значения параметра **Срок хранения**, которое вы задали для хранилища.

   Перед тем как выполнять восстановление архивных данных, убедитесь, что значение параметра **Срок хранения** перекрывает дату из поля Timestamp. В противном случае, архивные данные будут удалены в течение 1 часа.

2. Поместите архивную партицию в раздел detached вашего хранилища и распакуйте архив:

   `sudo unzip detached.zip -d <путь к каталогу detached>`

   Например:

   `sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/`

3. Выполните команду подключения партиции:

   ```
   sudo /opt/kaspersky/kuma/storage/<идентификатор хранилища>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<идентификатор партиции>'"
   ```

   `Повторите шаги распаковки архива и подключения партиции на каждой реплике шарда.`

В результате архивная партиция подключена и события снова доступны для поиска.

Создание набора ресурсов для хранилища

Сервис хранилища в веб-интерфейсе LogAnalyzer создается на основе набора ресурсов для хранилища.

Чтобы создать набор ресурсов для хранилища в веб-интерфейсе LogAnalyzer:

1. В веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Хранилища** нажмите **Добавить хранилище**.

   Откроется окно **Создание хранилища**.

2. На вкладке **Основные параметры** в поле **Название хранилища** введите уникальное имя создаваемого сервиса. Имя должно содержать от 1 до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.

4. В раскрывающемся списке **Теги** выберите теги для создаваемого набора ресурсов.

   В списке отображаются все доступные теги, созданные в тенанте ресурса и Общем тенанте. Вы может найти тег в списке, начав вводить его название в поле. Если тега, который вы ввели, не существует, вы можете нажать **Enter** или **Добавить**, чтобы создать его.

5. В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

6. В поле **Варианты условий хранения** выберите для хранилища условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно. Условие будет применено к пространству по умолчанию и к событиям из удаленных пространств.

   По умолчанию ClickHouse перемещает события на диски холодного хранения или удаляет их, если заполнено более 97% хранилища. В LogAnalyzer 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 2 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.

   - 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, направив 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 LogAnalyzer 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 LogAnalyzer получается со всех доступных реплик.
2. Если занятое пространство превышает установленные значения, LogAnalyzer 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, зарезерированное 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 LogAnalyzer (TTL).

7. Если вы хотите использовать дополнительное условие хранения, нажмите на кнопку **Добавить условие хранения** и укажите дополнительное условие хранения, как описано в пункте 6.

   Вы можете добавить не более двух условий и сочетать только условия следующих типов:

   - дни и размер хранилища в ГБ;
   - дни и размер хранилища в процентах.

   Если вы хотите удалить условие хранения, нажмите на значок крестика возле этого условия.

8. В поле **Срок хранения событий аудита** укажите, в течение какого количества дней вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: `365`.

9. При необходимости холодного хранения данных введите сроки хранения событий:

   - **Время хранения событий** – общая длительность хранения событий в LogAnalyzer 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 LogAnalyzer.

     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.

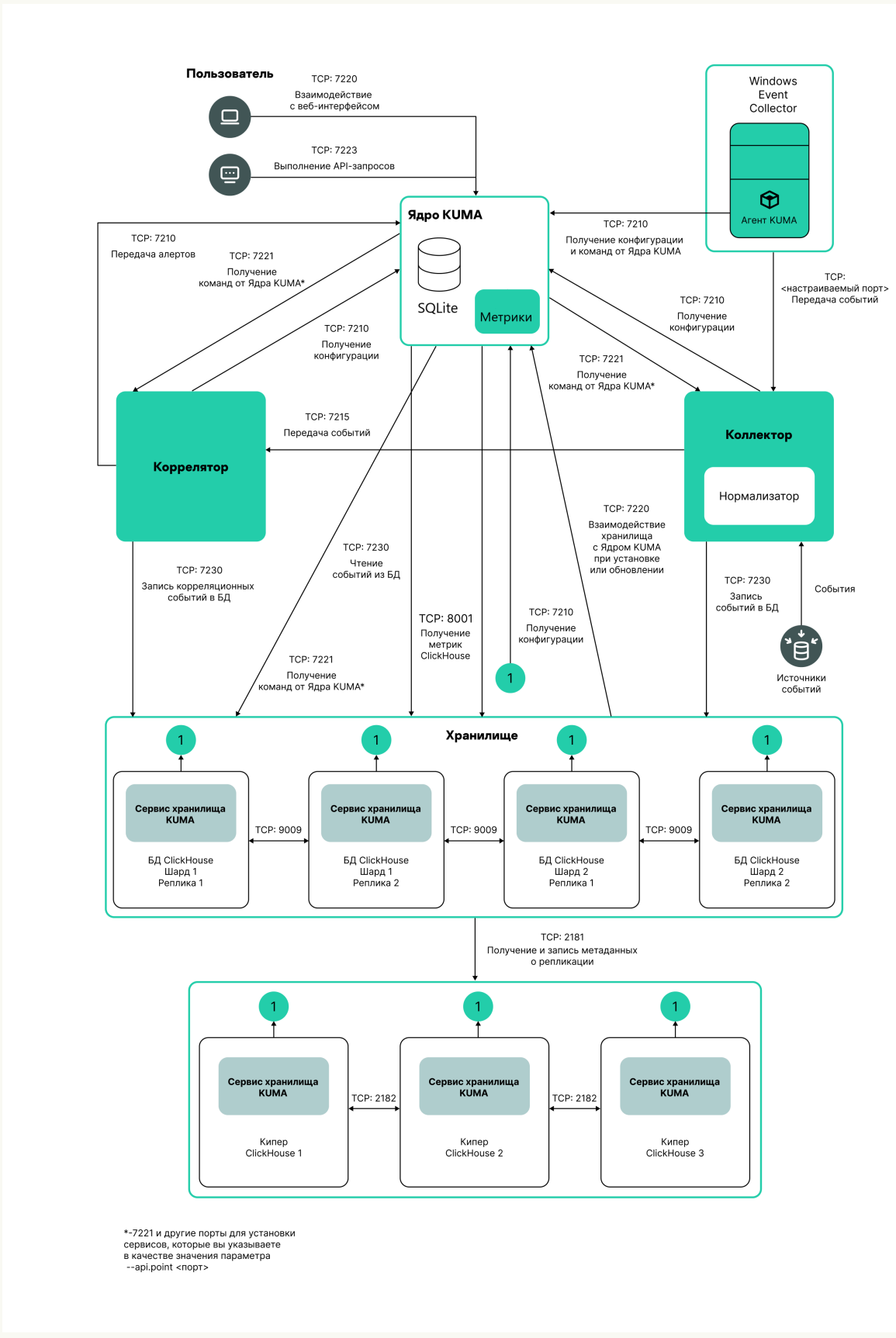


Схема распределенной установки

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 LogAnalyzer 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 (по данным VictoriaMetrics), 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 LogAnalyzer 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 LogAnalyzer.

  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

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.
- **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 LogAnalyzer.

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 **Полное доменное имя** 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.
    - В поле **Название** укажите название диска. Название должно содержать от 1 до 128 символов в кодировке Unicode.
    - 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 LogAnalyzer.

    - Если в качестве типа доменного имени диска вы выбрали **HDFS**, в поле **Хост** введите путь к HDFS. Например: `hdfs://hdfs1:9000/clickhouse/`.

15. 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 LogAnalyzer 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 LogAnalyzer будет ждать заполнения буфера. Если буфер не заполнен, но указанное время прошло, LogAnalyzer 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: в коллекторе 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 LogAnalyzer

Когда набор ресурсов для хранилища создан, можно перейти к созданию сервиса хранилища в LogAnalyzer.

Чтобы создать сервис хранилища в веб-интерфейсе LogAnalyzer:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer

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 LogAnalyzer>:<порт, используемый Ядром LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса LogAnalyzer> --install
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --id XXXXX --install`

   При развертывании нескольких сервисов LogAnalyzer 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.

Создание маршрутизатора событий

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Маршрутизатор событий – это сервис, который позволяет принимать потоки событий от коллекторов 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.

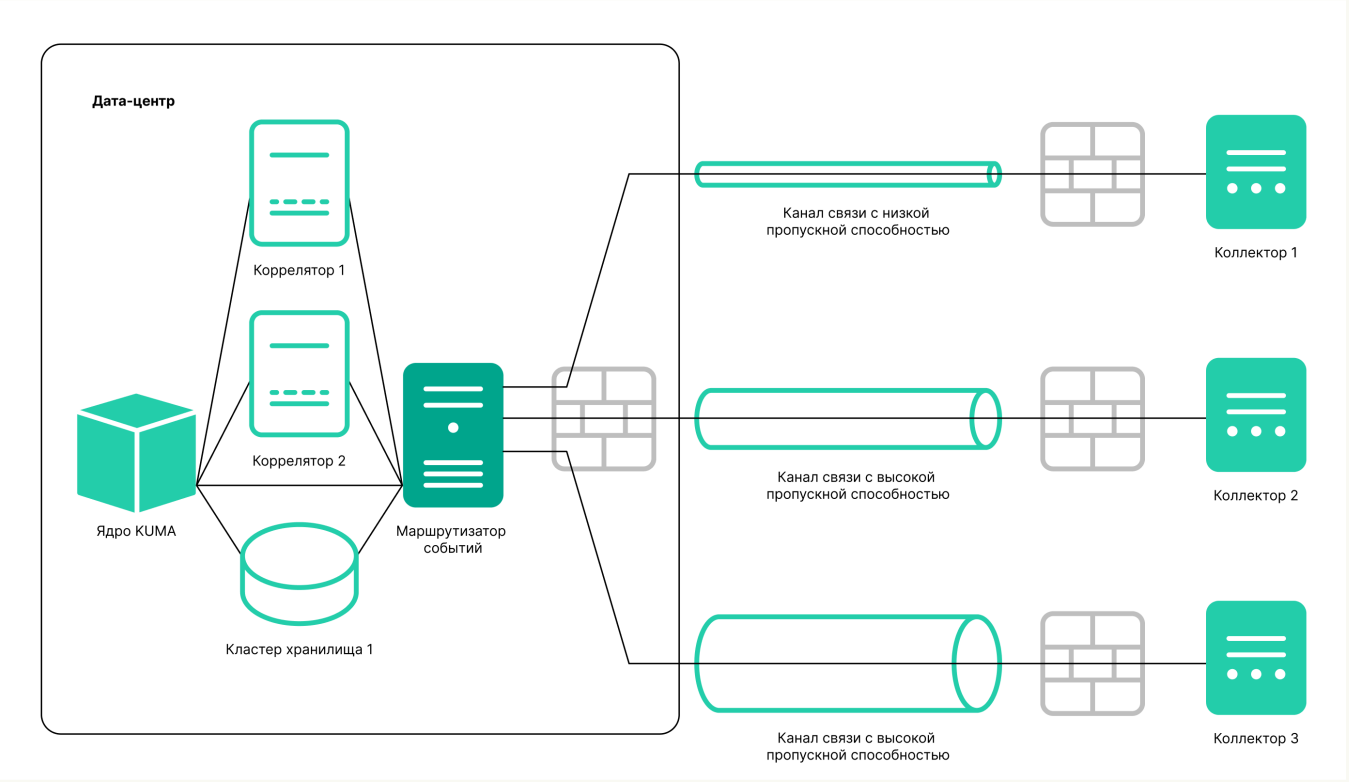
Создать маршрутизатор можно в разделе **Ресурсы**.

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 заданную точку назначения хранилища.



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. 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 в хранилище в дата-центре.

Маршрутизация в хранилище 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: коррелляторы и хранилище.

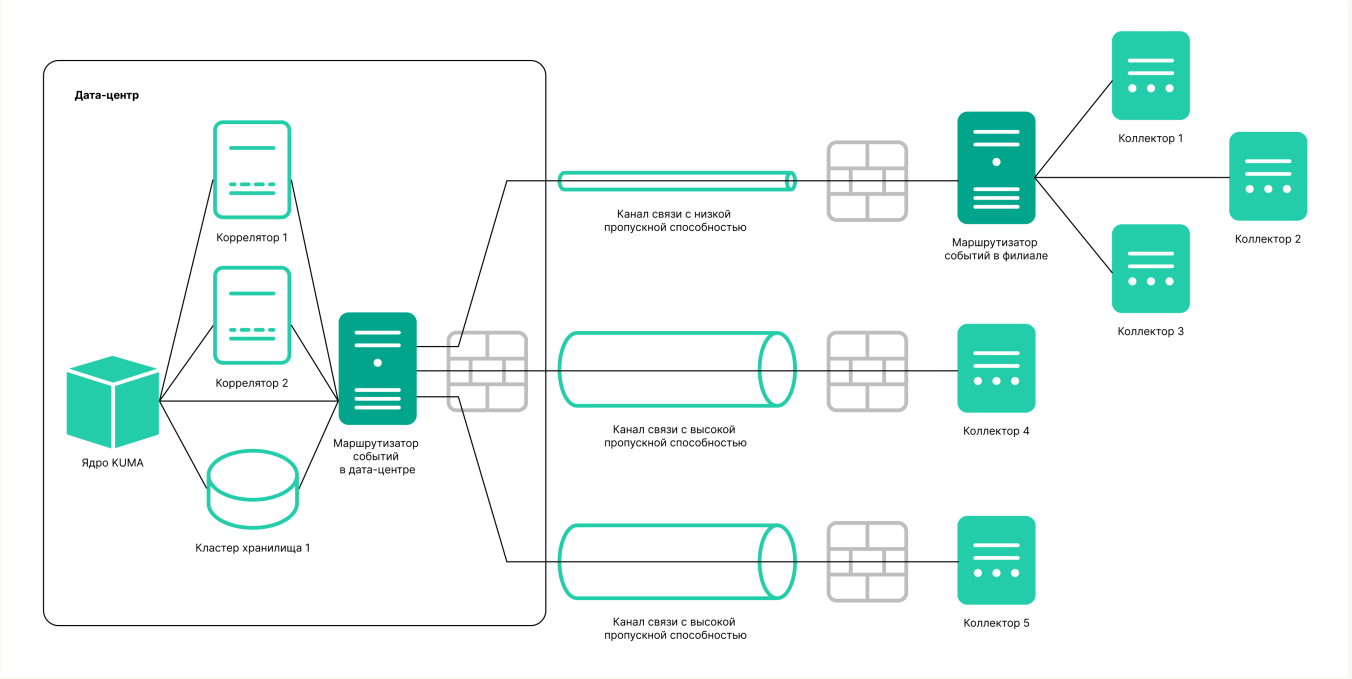


Схема каскадного подключения маршрутизаторов

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. Поскольку для маршрутизатора событий в файле инвентаря отсутствует отдельная секция, вы можете указать хост для установки маршрутизатора событий в секции `kuma_collector`. Также если вы планируете устанавливать маршрутизатор событий на отдельном хосте, вам нужно указать этот хост в файле инвентаря в секции `kuma_collector`, тогда при очередном обновлении LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 в точку назначения хранилища 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 LogAnalyzer, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Следует убедиться в сетевой связности LogAnalyzer и при необходимости открыть порты, используемые компонентами программы.

2. Закройте мастер, нажав **Сохранить**.

Сервис будет установлен в веб-интерфейсе LogAnalyzer. Теперь вы можете перейти к установке сервиса в сетевой инфраструктуре LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer в исключения брандмауэра.

   Для правильной работы программы убедитесь, что компоненты LogAnalyzer могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer

Создание коллектора в веб-интерфейсе LogAnalyzer 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 LogAnalyzer,

Запустите мастер установки коллектора:

- В веб-интерфейсе LogAnalyzer в разделе **Ресурсы** нажмите на кнопку **Подключить источник**.
- В веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

В результате выполнения шагов мастера в веб-интерфейсе LogAnalyzer 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 (задается отправка событий в хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коллектора LogAnalyzer

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 LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer в разделе **Ресурсы** нажмите **Подключить источник**.
- В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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:

   - tcp.
   - udp.
   - nats-jetstream.
   - kafka.
   - http.
   - sql.
   - file.
   - 1c-log.
   - 1c-xml.
   - diode.
   - ftp.
   - nfs.
   - wmi.
   - wec.
   - etw.
   - snmp.
   - snmp-trap.
   - kata\edr.
   - vmware.
   - elastic.

   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 LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer 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.

LogAnalyzer 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.

- **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 LogAnalyzer, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна.

- **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 корректность 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 LogAnalyzer:

   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 LogAnalyzer.

      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 LogAnalyzer, 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 LogAnalyzer название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:

- `$kuma_fileSourceName` – передать в поле события LogAnalyzer название обрабатываемого коллектором файла.
- `$kuma_fileSourcePath` – передать в поле события LogAnalyzer 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 LogAnalyzer. Вы можете найти поле события LogAnalyzer, введя его названия. Если название поля события LogAnalyzer начинается с `DeviceCustom*` и `Flex*`, при необходимости в поле **Подпись** укажите уникальную пользовательскую метку.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события LogAnalyzer.

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 LogAnalyzer, 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 LogAnalyzer, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если 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 LogAnalyzer. 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**.

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 LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer **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 LogAnalyzer **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 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 свернуть дочерние элементы с помощью кнопки или развернуть с помощью кнопки . Кнопки появятся, 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 LogAnalyzer 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.

- **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

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.

- **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.

Поступающие события сначала обогащаются данными из источников, которые вы выбираете на данном 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.

Обогащение с помощью правил обогащения

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ×. Можно использовать существующие правила обогащения или же создать правила непосредственно в мастере установки.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коллектора.

Чтобы создать в наборе ресурсов правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. 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 LogAnalyzer, 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** (доступно только в коммерческой версии LogAnalyzer)

  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 LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer, 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 (доступно только в коммерческой версии LogAnalyzer)
```

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 LogAnalyzer.
- **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 LogAnalyzer 3.4.1. С помощью переключателя можно включить отправку коллектором LogAnalyzer рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace** (доступно только в коммерческой версии LogAnalyzer)

  Для систем с большой нагрузкой на коллектор 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]**), LogAnalyzer 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 LogAnalyzer. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро LogAnalyzer.
  - **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 LogAnalyzer с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий LogAnalyzer, 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** (доступно только в коммерческой версии LogAnalyzer)

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 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), 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главный администратор также должен принять дополнительное лицензионное соглашение KSN в разделе **Kaspersky Security Network** (**Параметры** → **Интеграции** → **AI-сервисы** → **Kaspersky Security Network**).

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 берётся 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 LogAnalyzer 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, LogAnalyzer 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, LogAnalyzer 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 умочанию: `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 со списком параметров, которые нужно отправить в запросе в KSN для получения заключения, и списком соответствующих полей событий LogAnalyzer. 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, LogAnalyzer 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, LogAnalyzer 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.

  - **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize.

  Для каждого обязательного параметра укажите в таблице соответствующее ему поле события LogAnalyzer.

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 ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

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.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (**и**, **или**, **не**), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**. Вы можете просмотреть параметры вложенного фильтра, нажав на кнопку .

В набор ресурсов для коллектора добавлено новое правило обогащения.

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 точку назначения хранилища 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:

      - nats-jetstream
      - tcp
      - http
      - kafka
      - file
      - storage
      - 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 LogAnalyzer 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 программы LogAnalyzer – 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 LogAnalyzer> --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 LogAnalyzer, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы LogAnalyzer и при необходимости открыть используемые ее компонентами порты.

2. Закройте мастер, нажав **Сохранить коллектор**.

Сервис коллектора создан в LogAnalyzer. 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 LogAnalyzer.

Установка коллектора в сетевой инфраструктуре LogAnalyzer

Коллектор состоит из двух частей: одна часть создается в веб-интерфейсе LogAnalyzer, 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 LogAnalyzer>:<порт, используемый Ядром LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса LogAnalyzer> --api.port <порт, используемый для связи с устанавливаемым компонентом>`

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://test.kuma.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 LogAnalyzer 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 LogAnalyzer, идентификатор устанавливаемого коллектора, а также порт, который этот коллектор использует для связи.

> При развертывании нескольких сервисов LogAnalyzer 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 LogAnalyzer.

3. Выполните команду повторно, добавив ключ `--install`:

   `sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра LogAnalyzer>:<порт, используемый Ядром LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса LogAnalyzer> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install`

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

4. Добавьте порт коллектора LogAnalyzer в исключения брандмауэра.

> Для правильной работы программы убедитесь, что компоненты LogAnalyzer могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer:*

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в LogAnalyzer.

3. Убедитесь, что в разделе **Ресурсы** веб-интерфейса LogAnalyzer в раскрывающемся списке **Хранить исходное событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.

4. В разделе **События** в LogAnalyzer выполните поиск событий со следующими параметрами:

   - `ServiceID = <идентификатор коллектора, который требуется проверить>`
   - `Raw != ""`

   Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana™:

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в LogAnalyzer.
3. Откройте раздел Метрики и перейдите по ссылке LogAnalyzer 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 LogAnalyzer является важным условием защиты сетевой инфраструктуры. Бесперебойность можно обеспечить автоматическим перенаправлением потока событий на большее число коллекторов:

- На стороне LogAnalyzer 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 LogAnalyzer 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

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Агент LogAnalyzer состоит из двух частей: одна часть создается внутри веб-интерфейса LogAnalyzer, а вторая устанавливается на сервере или устройстве сетевой инфраструктуры.

Создание агента производится в несколько этапов:

1. **Создание набора ресурсов агента в веб-интерфейсе LogAnalyzer**
2. **Создание сервиса агента в веб-интерфейсе LogAnalyzer**
3. **Установка серверной части агента на устройстве, с которого требуется передавать события**

Агенты LogAnalyzer для устройств Windows можно создать следующим образом:

- Создать вручную путем создания набора ресурсов агента и создания сервиса агента в веб-интерфейсе LogAnalyzer.

- 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 LogAnalyzer 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 LogAnalyzer:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer

Когда набор ресурсов для агента создан, можно перейти к созданию сервиса агента в LogAnalyzer.

Чтобы создать сервис агента в веб-интерфейсе LogAnalyzer:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer

Когда сервис агента создан в LogAnalyzer, 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 LogAnalyzer на устройствах Linux

Агент LogAnalyzer, установленный на устройствах Linux, останавливается при закрытии терминала или при перезапуске сервера. Если вы не хотите запускать агентов LogAnalyzer вручную, мы рекомендуем устанавливать их с помощью программы, которая автоматически запускает программы при перезапуске сервера, например с помощью программы Supervisor. Если вы хотите запускать агентов LogAnalyzer автоматически, укажите в конфигурационном файле LogAnalyzer 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_<имя агента LogAnalyzer>] command=sudo /opt/kaspersky/kuma/agent agent
--core https://<FQDN сервера Ядра LogAnalyzer>:<номер порта Ядра LogAnalyzer>
autostart=true
autorestart=true
```

Чтобы установить агент LogAnalyzer на устройство Linux:

1. На устройстве Linux, на котором вы хотите установить агент LogAnalyzer, создайте директории для конфигурационного файла и агентов LogAnalyzer, например:
   - /opt/kaspersky/kuma;
   - /opt/kaspersky/agent.
2. Поместите конфигурационный файл LogAnalyzer в созданную для него директорию. Конфигурационный файл LogAnalyzer расположен внутри установщика в директории /kuma-ansible-installer/roles/kuma/files.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

3. Создайте пользователя LogAnalyzer выполнив команду:

   ```
   sudo useradd --system kuma && usermod -s /usr/bin/false kuma
   ```

4. Предоставьте пользователю LogAnalyzer доступ к директории с конфигурационным файлом LogAnalyzer, а также ко всем файлам внутри директории, выполнив команду:

   ```
   sudo chown -R kuma:kuma <путь к директории с конфигурационным файлом LogAnalyzer>
   ```

5. Установите агент LogAnalyzer, выполнив команду:

   ```
   sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN сервера Ядра LogAnalyzer>:<номер порта Ядра LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса LogAnalyzer> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента LogAnalyzer. Если не указать этот параметр, файлы будут храниться в директории, где расположен файл LogAnalyzer> [--accept-eula]
   ```

   Вы можете установить два агента LogAnalyzer на одном устройстве Linux. В этом случае агенты LogAnalyzer будут работать параллельно. При установке второго агента LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer.

   Примеры установки агента LogAnalyzer:

   - Установка агента LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, вы подтверждаете, что согласны с условиями Лицензионного соглашения и принимаете их.

6. Если вы выбрали установку LogAnalyzer с автоматическим принятием Лицензионного соглашения и хотите ознакомиться текстом лицензии или в процессе установки вам не был автоматически предоставлен текст Лицензионного соглашения, выполните команду:

   ```
   ./kuma license --show
   ```

Агент LogAnalyzer будет установлен на устройстве Linux.

Вы можете настроить коллектор для приема данных, которые агент LogAnalyzer пересылает в LogAnalyzer.

Установка агента LogAnalyzer на устройствах Windows

Перед установкой агента LogAnalyzer на устройстве Windows убедитесь, что учетная запись, под которой будет запускаться агент LogAnalyzer, обладает необходимыми правами.

Права для учетной записи при установке агента LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer) и только чтение журналов под доменной учетной записью, будет достаточно права Event Log Readers.

Права для учетной записи при установке агента LogAnalyzer 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 LogAnalyzer

Чтобы установить агент LogAnalyzer 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 LogAnalyzer>:<порт, используемый сервером ядра LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в LogAnalyzer> --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 LogAnalyzer.

   Примеры:

   - Установка агента LogAnalyzer без автоматического принятия Лицензионного соглашения:

     `kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install`

   - Установка агента LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer. Агент пересылает события Windows в LogAnalyzer: 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 LogAnalyzer, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента LogAnalyzer с устройств Windows

Чтобы удалить агент LogAnalyzer 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 LogAnalyzer> --uninstall`

Указанный агент LogAnalyzer удален с устройства Windows. События Windows больше не отправляются в LogAnalyzer.

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 LogAnalyzer>:<порт, используемый сервером ядра LogAnalyzer для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в LogAnalyzer> --user <имя пользователя, под которым будет работать агент, включая домен>
```

Обновление агентов

При обновлении версий LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в LogAnalyzer. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов LogAnalyzer

Настройка компонентов LogAnalyzer 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 LogAnalyzer.

   На этом этапе необходимо создать набор ресурсов агента LogAnalyzer, 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 коннектор типа **sql**.
   - 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 LogAnalyzer 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 LogAnalyzer) в директорию внешнего сервера (где их считывает коллектор LogAnalyzer).
- 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 поддерживается работа с SQL.

При использовании указанной выше схемы невозможно администрирование агента через веб-интерфейс LogAnalyzer, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 <путь к конфигурационному файлу агента> --wd <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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer с устройств Windows

Чтобы удалить агент LogAnalyzer 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 LogAnalyzer> --uninstall`

   Указанный агент LogAnalyzer удален с устройства Windows. События Windows больше не отправляются в LogAnalyzer.

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 LogAnalyzer событий с машин Windows

Для передачи событий с машин Windows в LogAnalyzer используется связка агента и коллектора LogAnalyzer. Передача данных организована следующим образом:

1. Установленный на машине агент LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer.**

3. **Установка агента LogAnalyzer 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 LogAnalyzer.**

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 LogAnalyzer **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.

   LogAnalyzer 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 LogAnalyzer.
   - 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 LogAnalyzer.
   - Для действующего сервиса агента, открытого для редактирования, перезапустите сервис агента.

Файл со списком серверов для агентов WMI будет импортирован.

Настройка источников событий

В этом разделе представлена информация о настройке получения событий из разных источников.

Настройка получения событий Auditd

LogAnalyzer позволяет осуществлять мониторинг и проводить аудит событий Auditd на устройствах Linux.

Перед настройкой получения событий убедитесь, что вы создали коллектор LogAnalyzer для событий Auditd.

Настройка получения событий Auditd состоит из следующих этапов:

1. **Настройка коллектора LogAnalyzer 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 LogAnalyzer**

   Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе LogAnalyzer.

Настройка коллектора LogAnalyzer 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 LogAnalyzer см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка сервера источника событий с помощью сервиса rsyslog

Для передачи событий от сервера в коллектор LogAnalyzer 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. Отредактируйте файл настроек 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 настроек 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 LogAnalyzer.

Настройка получения событий KATA/EDR

Вы можете настроить получение событий программы Kaspersky Anti Targeted Attack Platform в SIEM-систему LogAnalyzer.

Перед настройкой получения событий убедитесь, что вы создали коллектор LogAnalyzer для событий KATA/EDR.

При создании коллектора в веб-интерфейсе LogAnalyzer убедитесь, что номер порта и тип коннектора совпадают с портом и протоколом, указанными в параметрах передачи событий Kaspersky Anti Targeted Attack Platform в LogAnalyzer.

Для получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Настройка получения событий KATA/EDR состоит из следующих этапов:

1. Настройка пересылки событий KATA/EDR
2. Установка коллектора LogAnalyzer в сетевой инфраструктуре
3. Проверка поступления событий KATA/EDR в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий KATA/EDR выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе LogAnalyzer. События Kaspersky Anti Targeted Attack Platform отображаются в таблице с результатами поиска как KATA.

Настройка передачи событий KATA/EDR в LogAnalyzer

Чтобы настроить передачу событий из программы Kaspersky Anti Targeted Attack Platform в LogAnalyzer:

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 LogAnalyzer.

   c. В поле **Порт** укажите номер порта подключения к коллектору LogAnalyzer.

   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 LogAnalyzer настроена.

Создание коллектора LogAnalyzer для получения событий KATA/EDR

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе LogAnalyzer для событий Kaspersky Anti Targeted Attack Platform.

Подробнее о процедуре создания коллектора LogAnalyzer см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе LogAnalyzer убедитесь, что номер порта соответствует порту, указанному в пункте 4c настроек для передачи событий Kaspersky Anti Targeted Attack Platform в LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка передачи событий Kaspersky Security Center в SIEM-систему LogAnalyzer

LogAnalyzer позволяет получать и передавать события от Сервера администрирования Kaspersky Security Center в SIEM-систему LogAnalyzer.

Настройка передачи и получения событий Kaspersky Security Center состоит из следующих этапов:

1. Настройка передачи событий Kaspersky Security Center.
2. Настройка коллектора LogAnalyzer.
3. Установка коллектора LogAnalyzer в сетевой инфраструктуре.
4. Проверка поступления событий Kaspersky Security Center в коллектор LogAnalyzer.

   Вы можете проверить, что экспорт событий из Сервера администрирования Kaspersky Security Center в SIEM-систему LogAnalyzer выполнен правильно, выполнив поиск связанных событий в веб-интерфейсе LogAnalyzer.

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 LogAnalyzer:

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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

Настройка коллектора LogAnalyzer 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 LogAnalyzer.

Чтобы настроить коллектор LogAnalyzer для событий Kaspersky Security Center:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer.

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.

   Если точка назначения **Хранилище** не добавлена, создайте ее.

6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора LogAnalyzer.

Установка коллектора LogAnalyzer для сбора событий Kaspersky Security Center

После завершения настройки коллектора для сбора событий Kaspersky Security Center в формате CEF требуется установить коллектор LogAnalyzer на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора LogAnalyzer см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий Kaspersky Security Center из MS SQL

LogAnalyzer позволяет получать информацию о событиях Kaspersky Security Center из базы данных MS SQL (далее MS SQL).

Перед настройкой убедитесь, что вы создали коллектор LogAnalyzer для событий Kaspersky Security Center из MS SQL.

При создании коллектора в веб-интерфейсе LogAnalyzer 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 LogAnalyzer.

   Вы можете проверить, что настройка поступления событий из MS SQL выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе LogAnalyzer.

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 LogAnalyzer

После создания и настройки учетной записи в MS SQL требуется добавить секрет в веб-интерфейсе LogAnalyzer. Этот ресурс используется для хранения учетных данных для подключения к MS SQL.

Чтобы создать секрет в LogAnalyzer:

1. Откройте раздел веб-интерфейса LogAnalyzer **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 LogAnalyzer к БД MS SQL требуется настроить коннектор.

Чтобы настроить коннектор:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer для получения событий Kaspersky Security Center из MS SQL

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе LogAnalyzer для событий Kaspersky Security Center из MS SQL.

Подробнее о процедуре создания коллектора LogAnalyzer см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer на сервере сетевой инфраструктуры, предназначенной для получения событий.

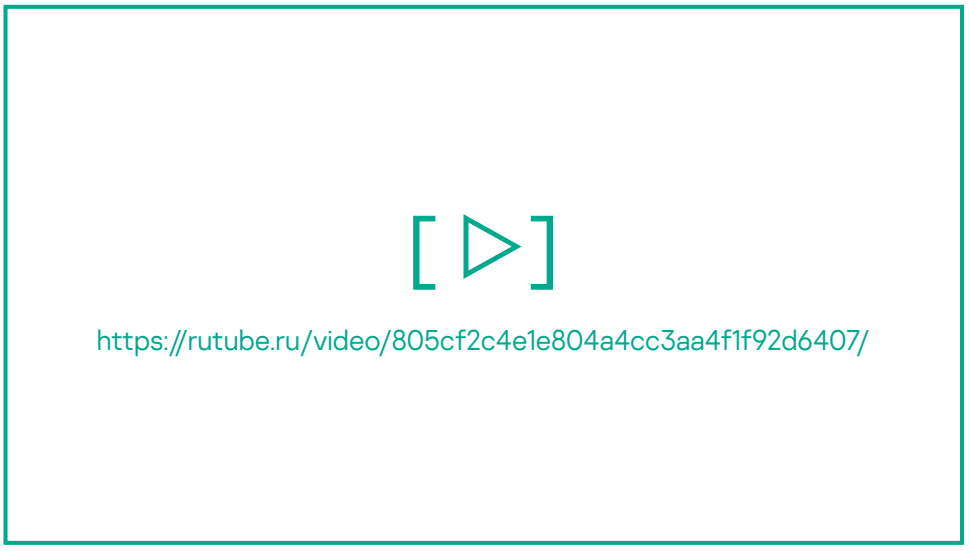
Подробнее о процедуре установки коллектора LogAnalyzer см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий с устройств Windows с помощью Агента LogAnalyzer (WEC)

LogAnalyzer позволяет получать информацию о событиях с устройств Windows с помощью Агента LogAnalyzer 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 LogAnalyzer.
6. Установка коллектора LogAnalyzer.
7. Передача в LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer для событий с устройств Windows.

Подробнее о процедуре создания коллектора LogAnalyzer см. в разделе Создание коллектора.

Для получения событий от устройств Windows в мастере установки коллектора LogAnalyzer 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.

   Если точка назначения **Хранилище** не добавлена, создайте ее.

6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора LogAnalyzer.

Установка коллектора LogAnalyzer для получения событий с устройств Windows

После завершения настройки коллектора для получения событий Windows требуется установить коллектор LogAnalyzer на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора LogAnalyzer см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка передачи в LogAnalyzer событий с устройств Windows с помощью Агента LogAnalyzer (WEC)

Чтобы завершить настройку передачи данных, требуется создать агент LogAnalyzer типа WEC, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Подробнее о создании и установке агента LogAnalyzer типа WEC на устройства Windows см. в разделе Передача в KUMA событий с устройств Windows.

Настройка получения событий с устройств Windows с помощью Агента LogAnalyzer (WMI)

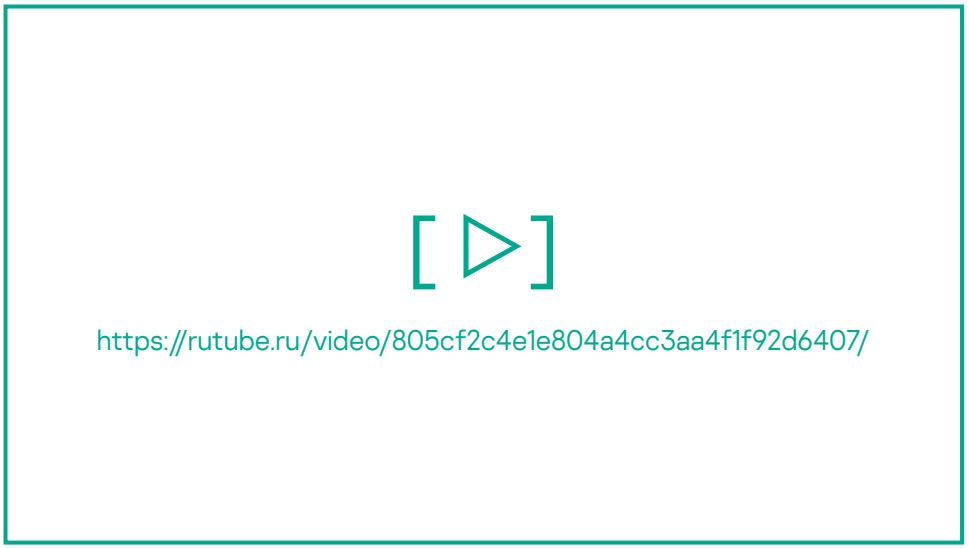
LogAnalyzer позволяет получать информацию о событиях с устройств Windows с помощью Агента LogAnalyzer типа WMI.

Настройка получения событий состоит из следующих этапов:

1. Настройка параметров аудита для работы с LogAnalyzer.
2. Настройка передачи данных с сервера источника событий.
3. Предоставление прав для просмотра событий.
4. Предоставление прав входа в качестве службы.
5. Создание коллектора LogAnalyzer.

   Для получения событий от устройств Windows в мастере установки коллектора LogAnalyzer на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Microsoft Products**.
6. Установка коллектора LogAnalyzer.
7. Передача в LogAnalyzer событий с устройств Windows.

   Чтобы завершить настройку передачи данных, требуется создать агент LogAnalyzer типа WMI, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.



Настройка параметров аудита для работы с LogAnalyzer

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 LogAnalyzer.

- *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 LogAnalyzer.

   При создании коллектора LogAnalyzer 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 LogAnalyzer будет ожидать соединения от агента LogAnalyzer. 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.

   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 LogAnalyzer на сервере.

3. Установка коллектора LogAnalyzer на сервере.

   Выполните следующие действия:

   a. Подключитесь к интерфейсу командной строки LogAnalyzer, используя учетную запись пользователя с правами root.

   b. Установите коллектор LogAnalyzer, выполнив команду, которую вы скопировали на 8-м шаге мастера установки коллектора.

   c. Если вы хотите добавить порт коллектора LogAnalyzer 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 LogAnalyzer будет установлен, и статус сервиса коллектора LogAnalyzer изменится на зеленый в веб-интерфейсе LogAnalyzer.

4. Создание агента LogAnalyzer.

   При создании агента LogAnalyzer 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 LogAnalyzer будет ожидать соединения от агента LogAnalyzer. 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 LogAnalyzer.

   Вам нужно скопировать идентификатор созданного сервиса агента LogAnalyzer. Для этого нажмите на правую кнопку мыши рядом с сервисом агента LogAnalyzer и в контекстном меню выберите пункт **Копировать идентификатор**.

6. Создание учетной записи для агента LogAnalyzer.

   Создайте доменную или локальную учетную запись Windows для запуска агента LogAnalyzer 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**).

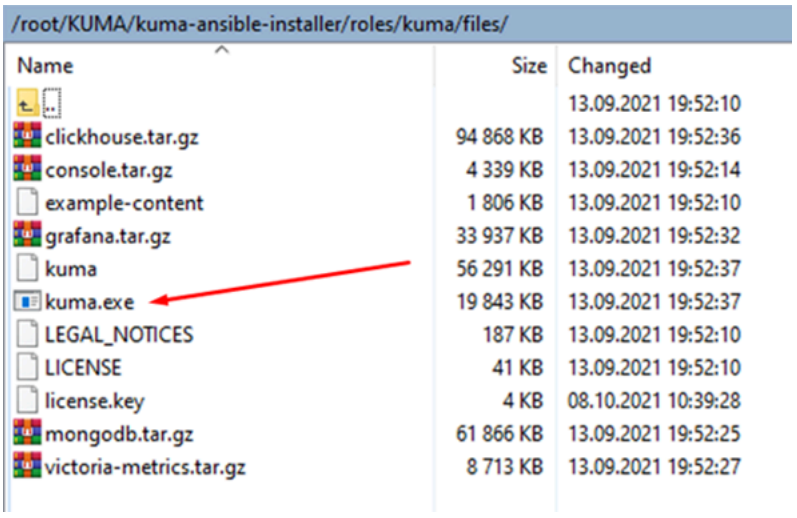
7. Установка агента LogAnalyzer на Windows-сервере.

Вам нужно установить агент LogAnalyzer на Windows-сервере, который будет обеспечивать прием событий от поставщика. Для этого выполните следующие действия:

a. Добавьте FQDN сервера LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer>
```

В веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** убедитесь, что сервис агента LogAnalyzer был запущен и его статус изменился на зеленый, после чего прервите выполнение команды.

f. Запустите установку агента LogAnalyzer одним из следующих способов:

- Если вы хотите запустить установку агента LogAnalyzer 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 LogAnalyzer> --user <домен>\<имя учетной записи для агента LogAnalyzer> --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 LogAnalyzer> --user <имя учетной записи для агента LogAnalyzer> --install
  ```

Вам потребуется ввести пароль учетной записи для агента LogAnalyzer.

На Windows-сервере будет установлен сервис KUMA Windows Agent <идентификатор сервиса агента LogAnalyzer>. Если в веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы** сервис агента LogAnalyzer не запущен и имеет красный статус, вам нужно убедиться в доступности портов 7210, а также порта коллектора Windows по направлению от агента LogAnalyzer к коллектору LogAnalyzer.

Для удаления сервиса агента LogAnalyzer на Windows-сервере выполните команду:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --id <идентификатор сервиса агента LogAnalyzer> --uninstall
```

8. Проверка поступления событий DNS-сервера в коллектор LogAnalyzer.

   Вы можете проверить, что настройка получения событий DNS-сервера с помощью коннектора ETW выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка на стороне Windows

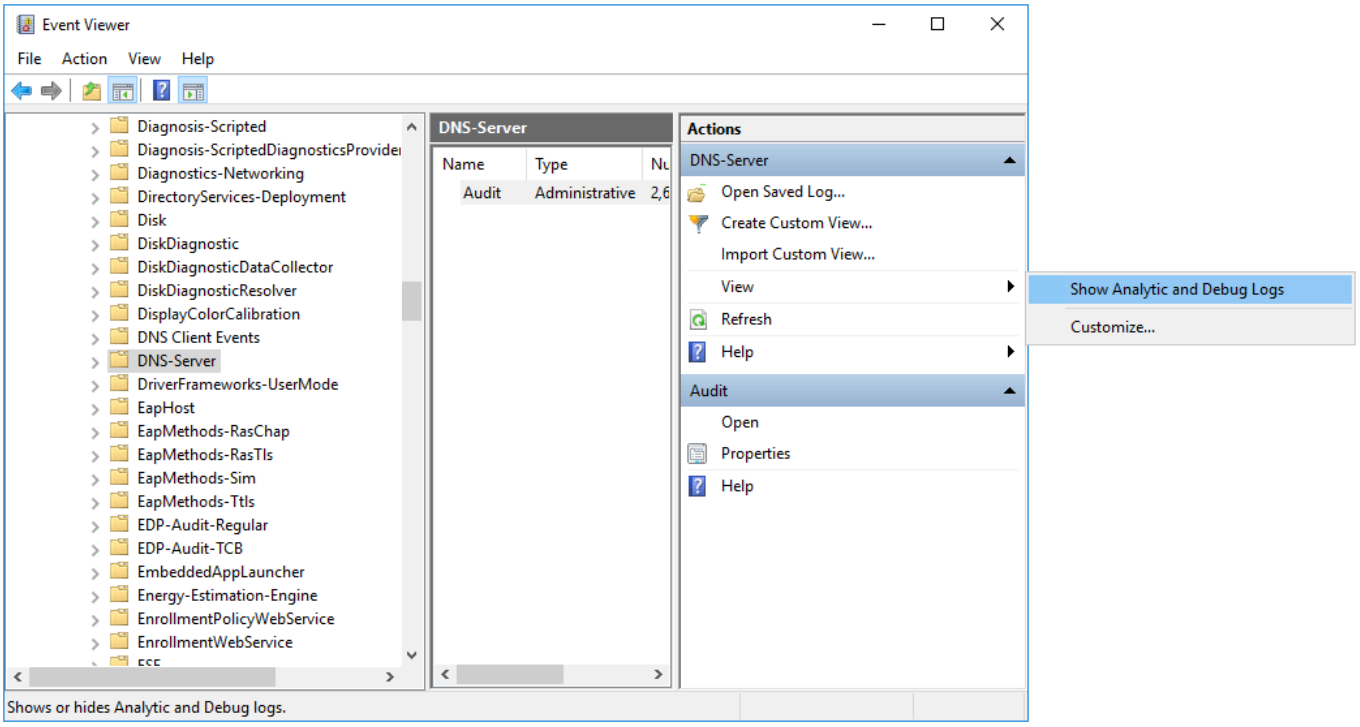
Чтобы настроить получение событий DNS-сервера с помощью коннектора ETW на стороне Windows:

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**.

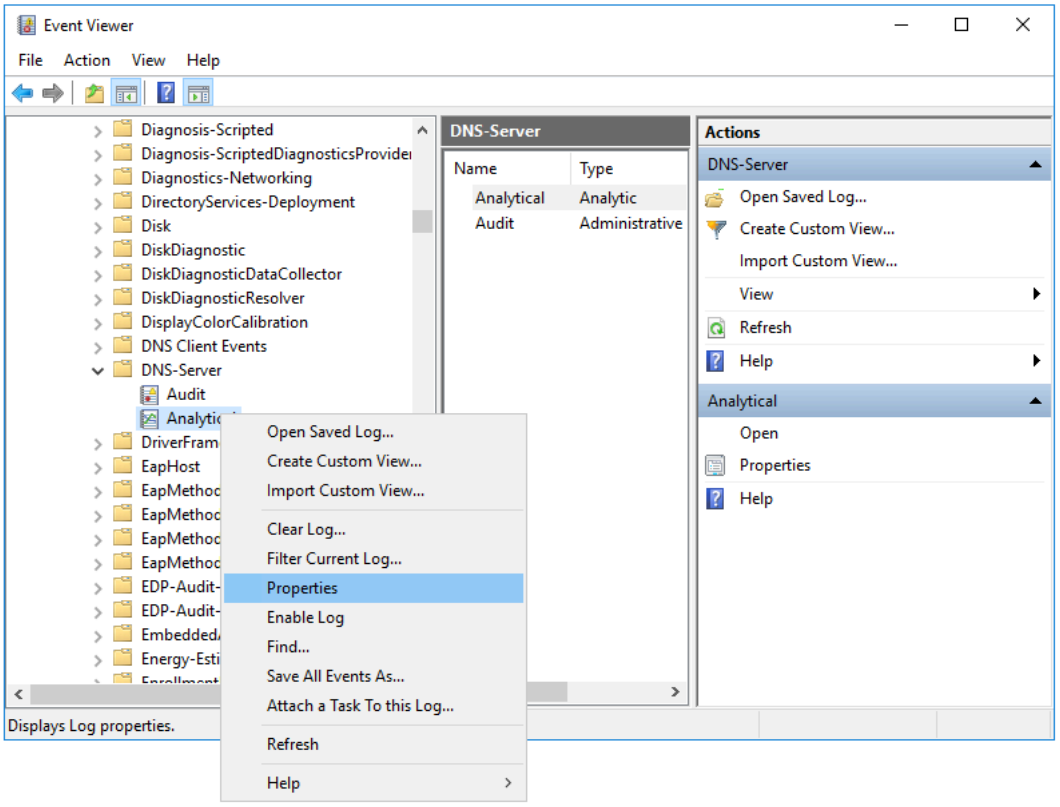


Отображение аналитического и отладочного журнала

Отобразится отладочный журнал **Audit** и аналитический журнал **Analytical**.

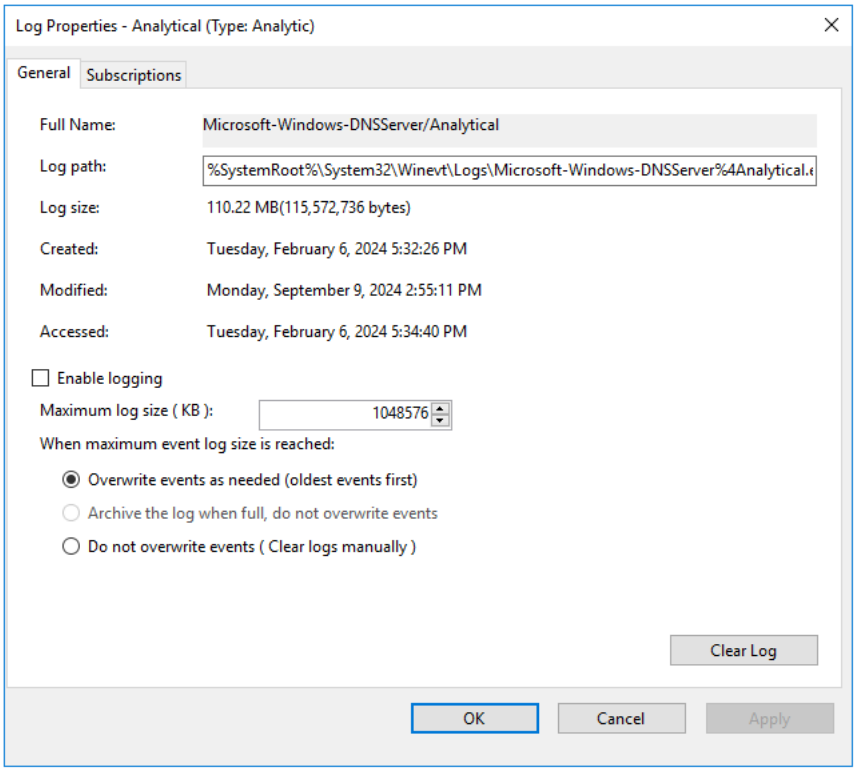
4. Настройте аналитический журнал:

a. Откройте контекстное меню аналитического журнала **Analytical** и выберите пункт **Свойства**.



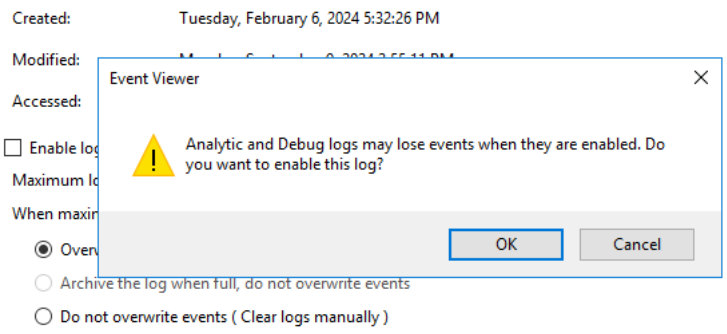
Переход в свойства аналитического журнала Analytical

a. В открывшемся окне убедитесь, что в поле **Макс. размер журнала (КБ)** указано значение `1048576`.



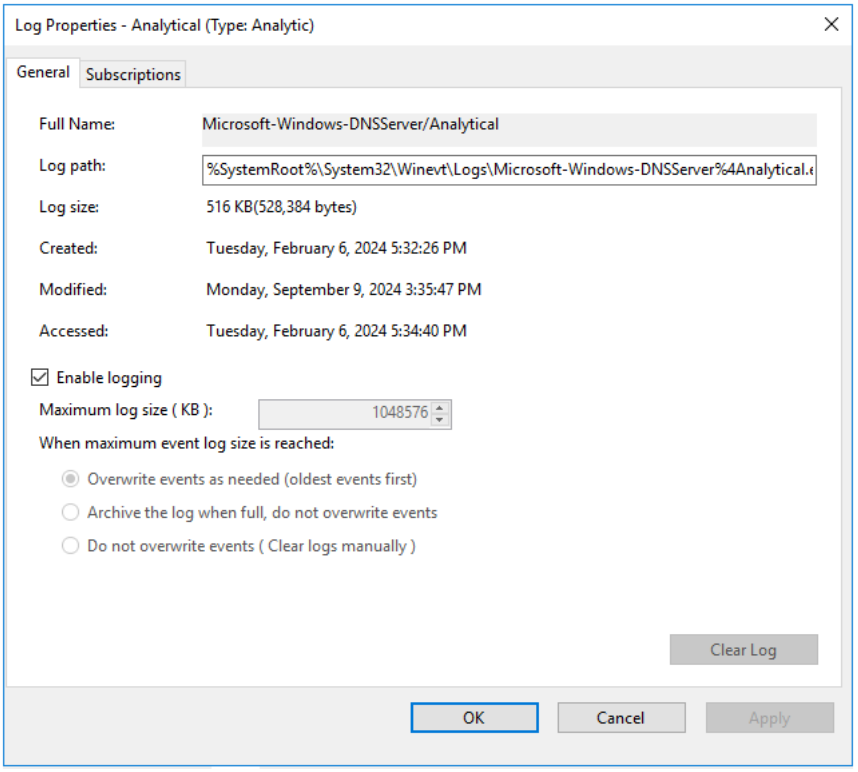
Свойства аналитического журнала Analytical

a. Установите флажок **Включить ведение журнала** и в открывшемся окне подтверждения нажмите на кнопку **OK**.



Окно подтверждения

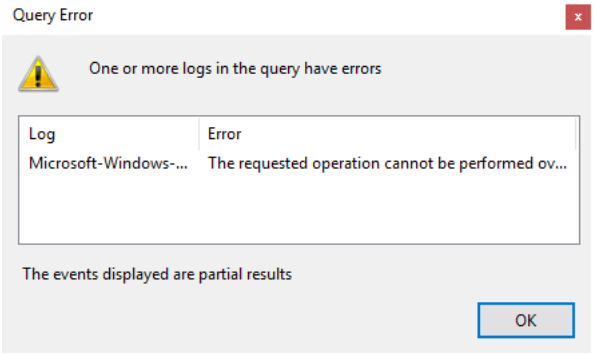
Параметры аналитического журнала должны быть настроены следующим образом:



Проверка корректности параметров аналитического журнала Analytical

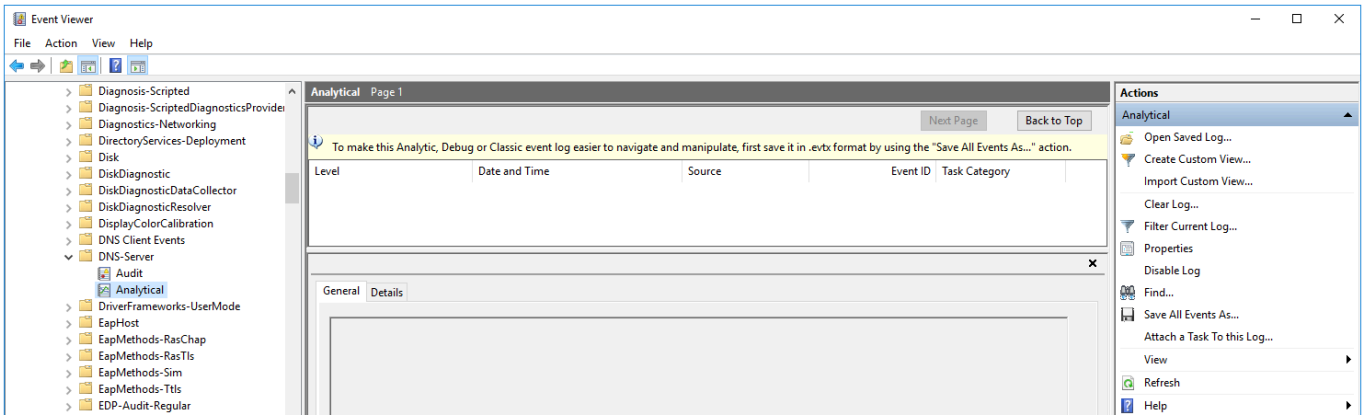
a. Нажмите на кнопку **Применить**, после чего нажмите на кнопку **OK**.

Отобразится окно с ошибкой.



Окно ошибки

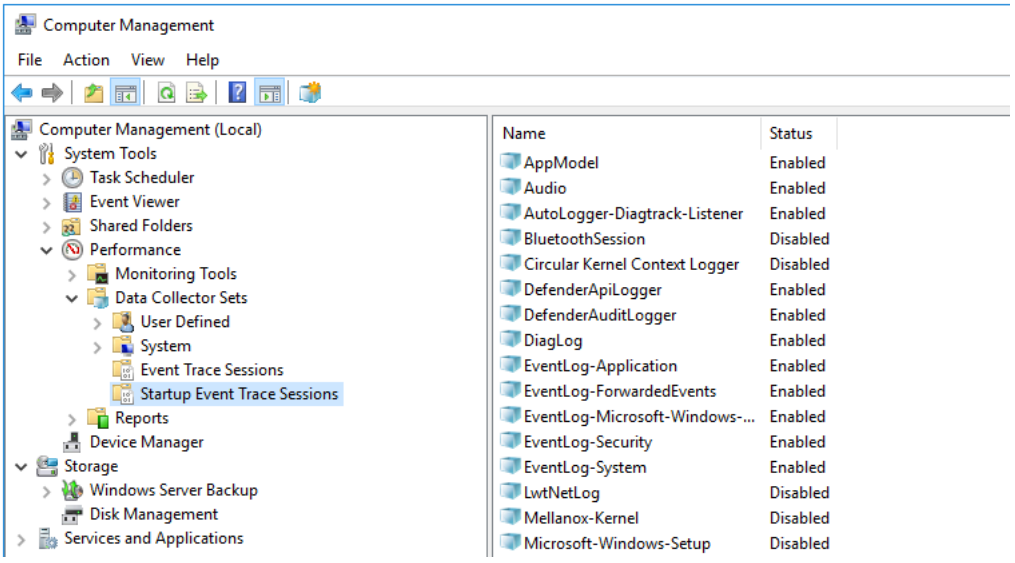
При включенной ротации аналитического журнала события не отображаются. Для просмотра событий в панели **Действия** нажмите на кнопку **Остановить журнал**.



Остановка журнала

5. Запустите Управление компьютером (англ. Computer management) от имени администратора.

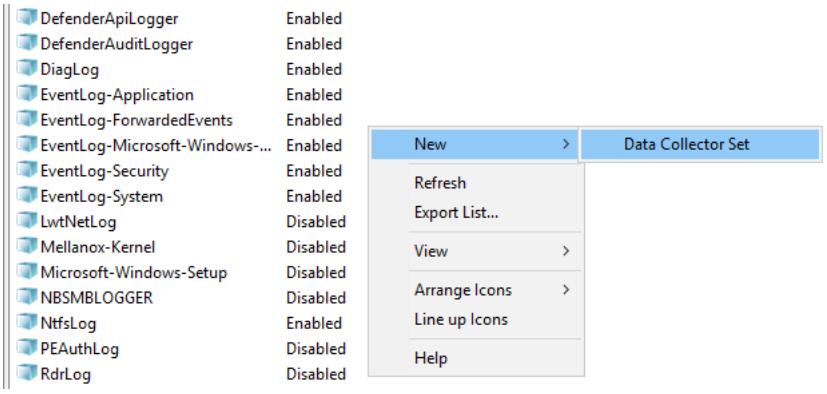
6. В открывшемся окне перейдите в директорию **Служебные программы** → **Производительность** → **Сеансы отслеживания событий запуска**.



Управление компьютером

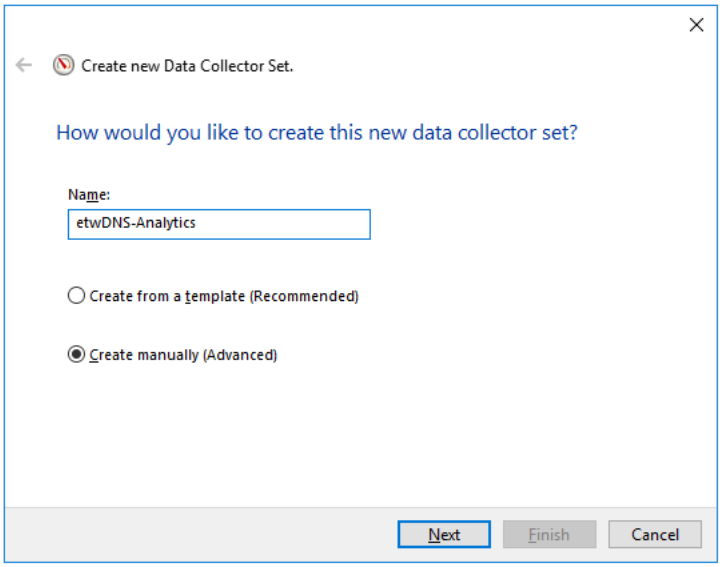
7. Создайте поставщика:

a. Откройте контекстное меню директории **Сеансы отслеживания событий запуска** и выберите пункт **Создать → Группа сборщиков данных**.



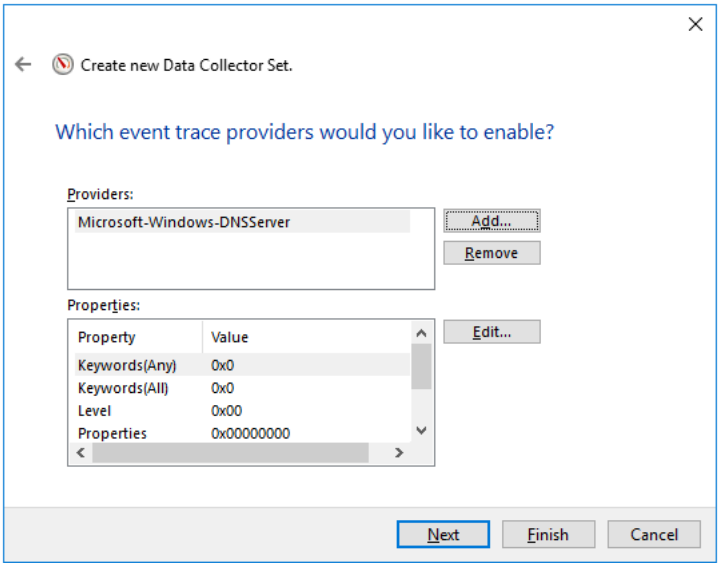
Создание группы сборщиков данных

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**.

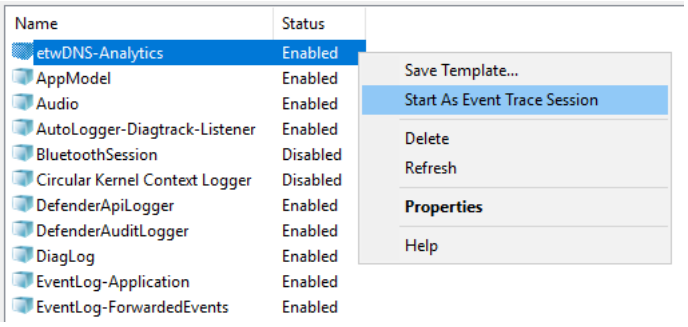


Выбор поставщика

Агент LogAnalyzer 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**.



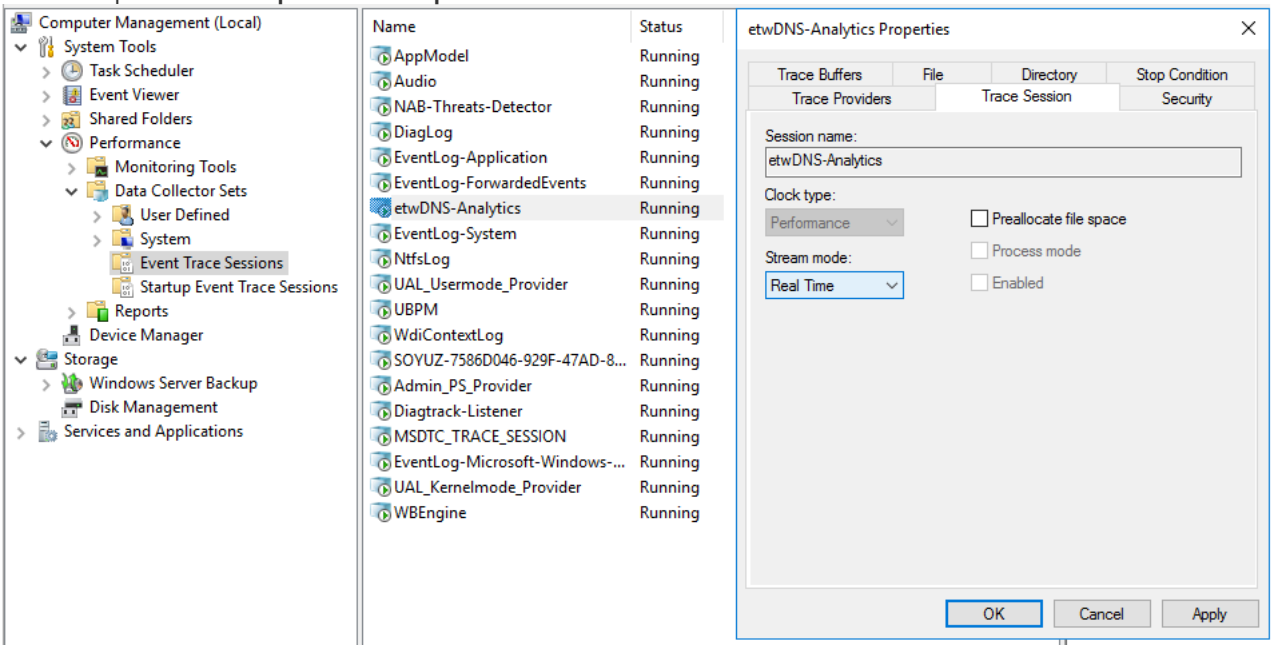
Запуск поставщика

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

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.
4. Настройка сервера источника событий.
5. Проверка поступления событий PostgreSQL в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий PostgreSQL выполнена правильно в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий ИВК Кольчуга-К в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий ИВК Кольчуга-К.
4. Проверка поступления событий ИВК Кольчуга-К в LogAnalyzer.

   Вы можете проверить, что настройка источника событий ИВК Кольчуга-К выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий ИВК Кольчуга-К в LogAnalyzer

Чтобы настроить передачу событий межсетевого экрана ИВК КОЛЬЧУГА-К по syslog в коллектор LogAnalyzer:

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 LogAnalyzer. 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий КриптоПро NGate в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий КриптоПро NGate.
4. Проверка поступления событий КриптоПро NGate в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий КриптоПро NGate выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий КриптоПро NGate в LogAnalyzer

Чтобы настроить передачу событий из программы КриптоПро NGate в LogAnalyzer:

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 LogAnalyzer.

Настройка получения событий Ideco UTM

Вы можете настроить получение событий программы Ideco UTM в LogAnalyzer по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Ideco UTM в LogAnalyzer.

2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий Ideco UTM.

4. Проверка поступления событий Ideco UTM в LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Ideco UTM выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий Ideco UTM в LogAnalyzer

Чтобы настроить передачу событий из программы Ideco UTM в LogAnalyzer:

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 LogAnalyzer.

4. В параметре Порт введите порт, который прослушивает коллектор LogAnalyzer.

5. Нажмите **Сохранить** для применения внесенных изменений.

Передача событий в Ideco UTM в LogAnalyzer будет настроена.

Настройка получения событий KWTS

Вы можете настроить получение событий из системы анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (KWTS) в LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KWTS в LogAnalyzer.

2. Создание коллектора LogAnalyzer для получения событий KWTS.

   Для получения событий KWTS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KWTS**.

3. Установка коллектора LogAnalyzer для получения событий KWTS.

4. Проверка поступления событий KWTS в коллектор LogAnalyzer.

   Вы можете проверить, что настройка передачи событий KWTS выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий KWTS в LogAnalyzer

Чтобы настроить передачу событий KWTS в LogAnalyzer:

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**.

Настройка получения событий KLMS

Вы можете настроить получение событий из системы анализа и фильтрации почтового трафика Kaspersky Linux Mail Server (KLMS) в SIEM-систему LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. В зависимости от используемой версии KLMS, выберите один из вариантов:
   - Настройка передачи событий KLMS 8 в LogAnalyzer.
   - Настройка передачи событий KLMS 10 в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий KLMS.
4. Проверка поступления событий KLMS в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий KLMS выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий KLMS в LogAnalyzer

Чтобы настроить передачу событий KLMS в LogAnalyzer:

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) 1.1 в SIEM-систему LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KSMG в LogAnalyzer.

2. Создание коллектора LogAnalyzer для получения событий KSMG.

   Для получения событий KSMG в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSMG**.

3. Установка коллектора LogAnalyzer для получения событий KSMG.

4. Проверка поступления событий KSMG в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий KSMG выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий KSMG в LogAnalyzer

Чтобы настроить передачу событий KSMG в LogAnalyzer:

1. Подключитесь к серверу KSMG по протоколу SSH под учетной записью с правами администратора.

2. С помощью утилиты ksmg-control выгрузите настройки в файл settings.xml:

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-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>
   ```

4. Примените настройки с помощью следующей команды:

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-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 KICS for Networks

Вы можете настроить получение событий из программы Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) версии 4.2 в LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Создание коннектора KICS for Networks для передачи событий в LogAnalyzer.
2. Настройка передачи событий KICS for Networks в LogAnalyzer.
3. Создание и установка коллектора LogAnalyzer для получения событий KICS for Networks.
4. Проверка поступления событий KICS for Networks в коллектор LogAnalyzer.

   Вы можете проверить, что настройка передачи событий KICS for Networks выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Создание коннектора KICS for Networks для передачи событий в LogAnalyzer

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 LogAnalyzer 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 LogAnalyzer.
   g. В поле **Номер порта** введите номер порта коллектора LogAnalyzer.
   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 LogAnalyzer будет готов к работе.

Настройка передачи событий KICS for Networks в LogAnalyzer

Чтобы события безопасности KICS for Networks передавались в LogAnalyzer:

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 LogAnalyzer.
4. Нажмите на кнопку **Выбрать коннекторы**.
5. В открывшемся окне выберите коннектор, созданный для передачи событий в LogAnalyzer.
6. Нажмите на кнопку **Ok**.

   Выбранные типы событий будут передаваться в LogAnalyzer. В таблице **Типы событий** эти типы событий отмечаются флажком в столбце с названием коннектора.

Создание коллектора LogAnalyzer для получения событий KICS for Networks

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе LogAnalyzer для событий KICS for Networks.

Подробнее о процедуре создания коллектора LogAnalyzer см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе LogAnalyzer 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.

   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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий PT NAD в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий PT NAD.

4. Проверка поступления событий PT NAD в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий PT NAD выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий PT NAD в LogAnalyzer

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

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] MariaDB Audit Plugin syslog**.
4. Установка коллектора в сетевой инфраструктуре LogAnalyzer.
5. Проверка поступления событий MySQL и MariaDB в коллектор LogAnalyzer.

   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 LogAnalyzer>:<порт коллектора LogAnalyzer>`

   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

LogAnalyzer позволяет получать информацию о событиях Apache Cassandra.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Apache Cassandra в LogAnalyzer.
2. Создание коллектора LogAnalyzer для событий Apache Cassandra.

   Для получения событий Apache Cassandra в мастере установки коллектора LogAnalyzer 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 LogAnalyzer.
4. Проверка поступления событий Apache Cassandra в коллектор LogAnalyzer.

   Чтобы проверить, что настройка сервера источника событий Apache Cassandra выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка журналирования событий Apache Cassandra в LogAnalyzer

Чтобы настроить журналирование событий Apache Cassandra в LogAnalyzer:

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 LogAnalyzer по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий FreeIPA в LogAnalyzer.
2. Создание коллектора LogAnalyzer для получения событий FreeIPA.

   Для получения событий FreeIPA в мастере установки коллектора LogAnalyzer на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] FreeIPA**.
3. Установка коллектора LogAnalyzer в сетевой инфраструктуре.
4. Проверка поступления событий FreeIPA в LogAnalyzer.

   Чтобы проверить, что настройка сервера источника событий FreeIPA выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка передачи событий FreeIPA в LogAnalyzer

Чтобы настроить передачу событий FreeIPA в LogAnalyzer 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 LogAnalyzer по протоколу syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий VipNet TIAS в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий VipNet TIAS.

4. Проверка поступления событий VipNet TIAS в LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий VipNet TIAS выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка передачи событий VipNet TIAS в LogAnalyzer

Чтобы настроить передачу событий VipNet TIAS в LogAnalyzer 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 LogAnalyzer.

      Например, 10.1.2.3 или syslog.siem.ru

   2. В поле **Порт** укажите входящий порт коллектора LogAnalyzer. По умолчанию указан порт 514.

   3. В списке **Протокол** выберите протокол транспортного уровня, который прослушивает коллектор LogAnalyzer. 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 LogAnalyzer выполнена.

Настройка получения событий Nextcloud

Вы можете настроить получение событий программы Nextcloud 26.0.4 в SIEM-систему LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer для получения событий Nextcloud.
5. Проверка поступления событий Nextcloud в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Nextcloud выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка аудита событий Nextcloud

Чтобы настроить передачу событий Nextcloud в LogAnalyzer:

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 LogAnalyzer 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Snort.

2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий Snort.

4. Проверка поступления событий Snort в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Snort выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Suricata в LogAnalyzer.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий Suricata.

4. Проверка поступления событий Suricata в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Suricata выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий FreeRADIUS.

2. Настройка Syslog-сервера для отправки событий FreeRADIUS.

3. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий FreeRADIUS.

5. Проверка поступления событий FreeRADIUS в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий FreeRADIUS выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer будет настроена.

Настройка получения событий VMware vCenter

Вы можете настроить получение событий VMware vCenter в SIEM-систему LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка подключения к VMware vCenter.

2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий VMWare Vcenter.

4. Проверка поступления событий VMWare Vcenter в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий VMWare Vcenter выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий zVirt в LogAnalyzer.

2. Создание коллектора LogAnalyzer 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 LogAnalyzer для получения событий zVirt.

4. Проверка поступления событий zVirt в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий zVirt выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer:

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 LogAnalyzer>: <порт коллектора LogAnalyzer>`.

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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Преобразование формата журнала событий Zeek IDS.

   Нормализатор LogAnalyzer поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор LogAnalyzer файлы журналов нужно преобразовать в формат JSON.

2. Создание коллектора LogAnalyzer для получения событий Zeek IDS.

   Для получения событий Suricata в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] ZEEK IDS json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора LogAnalyzer для получения событий Zeek IDS.

4. Проверка поступления событий Zeek IDS в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Zeek IDS выполнена правильно, в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer. Это позволяет получить в LogAnalyzer события из журналов Windows (Kaspersky Endpoint Security for Windows версии 12.6–12.10 поддерживает ограниченный набор EventID продуктов компании Microsoft) со всех хостов, на которых установлен Kaspersky Endpoint Security for Windows версии 12.6 и выше, без установки агентов LogAnalyzer на эти хосты. Чтобы активировать функционал, необходимо:

- иметь действующую лицензию LogAnalyzer.
- 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 LogAnalyzer**

   В LogAnalyzer должно быть настроено получение обновлений через серверы обновлений "Лаборатории Касперского".

   Нажмите Импорт ресурсов и выберите **[OOTB] Microsoft Products via KES WIN** в списке доступных к установке нормализаторов.

2. **Создание коллектора LogAnalyzer для получения событий Windows**

   В зависимости от используемой версии Kaspersky Endpoint Security for Windows нужно выполнить следующие действия:

   - Если вы используете Kaspersky Endpoint Security for Windows версии 12.6–12.10, на шаге **Транспорт** нужно выбрать **TCP** или **UDP** и указать номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Microsoft Products via KES WIN** и на шаге **Фильтрация событий** нужно выбрать 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** нужно выбрать **TCP** или **UDP** и указать номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** нужно выбрать один из следующих вариантов:

     - Для LogAnalyzer версии 3.2–4.0 нужно выбрать нормализатор **[OOTB] Microsoft Products via KES WIN NG for KUMA 3.2**.

     - Для LogAnalyzer версии 4.0.1 и выше нужно выбрать нормализатор **[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 LogAnalyzer, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия LogAnalyzer и используется Kaspersky Endpoint Security for Windows версии 12.6. Мы планируем активировать функционал отправки журналов Windows в коллектор LogAnalyzer. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям LogAnalyzer не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено 2 ключа с лицензиями для LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer и настроить сетевые параметры подключения.

5. **Проверка поступления событий Windows в коллектор LogAnalyzer**

   Вы можете проверить, что настройка сервера источника событий Windows выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

   Перечень событий продуктов Microsoft, которые Kaspersky Endpoint Security for Windows версии 12.6–12.10 передает в LogAnalyzer, приведен в следующей таблице:

Журнал событий	Идентификатор события
System	12 13 7040 7045 42 104 107 109 1074 6005 6006 7034 7036 8003
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

Журнал событий	Идентификатор события
	5632
	5888
	5890
	6416
	4622
	4648
	4672
	4697
	4702
	4719
	4732
	4733
	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

Журнал событий	Идентификатор события
	4755 4758 4759 4760 4761 4762 4763 4764 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

Журнал событий	Идентификатор события
	5024 5031 5033 5039 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 for Linux, начиная с версии 12.2, есть возможность отправлять события из журналов Linux в коллектор LogAnalyzer. Это позволяет получить в LogAnalyzer события из журналов Linux со всех хостов, на которых установлен Kaspersky Endpoint Security for Linux версии 12.2. Чтобы активировать функционал, необходимо:

- иметь действующую лицензию LogAnalyzer.
- использовать Kaspersky Security Center 14.2 и выше.
- использовать Kaspersky Endpoint Security for Linux 12.2 или выше.

Настройка получения событий состоит из следующих этапов:

1. Импорт нормализатора в LogAnalyzer.

   В LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия LogAnalyzer и используется Kaspersky Endpoint Security for Linux версии 12.2. Мы планируем активировать функционал отправки журналов Linux в коллектор LogAnalyzer. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям LogAnalyzer не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено 2 ключа с лицензиями для LogAnalyzer и для активирования функционала Kaspersky Endpoint Security for Linux.

   В ответ на письмо вам будет предоставлен файл ключа.

4. Настройка на стороне Kaspersky Security Center и Kaspersky Endpoint Security for Linux.

   Файл ключа, активирующий функционал отправки событий Linux в коллекторы LogAnalyzer, 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 LogAnalyzer и настроить сетевые параметры подключения.

5. Проверка поступления событий Linux в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Linux выполнена правильно, в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

   Kaspersky Endpoint Security for 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита системы Codemaster Mirada.
2. Создание коллектора LogAnalyzer 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 LogAnalyzer.
4. Проверка поступления событий Codemaster Mirada в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Codemaster Mirada выполнена правильно, в разделе **События** веб-интерфейса LogAnalyzer.

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 LogAnalyzer.
6. В поле **Протокол** укажите транспортный протокол **UDP** или **TCP**.
7. В поле **Порт** укажите порт, который прослушивает коллектор LogAnalyzer.

   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 LogAnalyzer. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP. Ресурсы, описанные в этой статье, доступны для LogAnalyzer 3.0 и более новых версий.

Настройка получения событий состоит из следующих этапов:

1. Настройка Postfix для отправки событий.
2. Настройка коллектора LogAnalyzer для получения событий Postfix.
3. Проверка поступления событий Postfix в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий Postfix выполнена правильно в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer, 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 в хранилище будет направлено одно событие.

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 затемагрегированные 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.

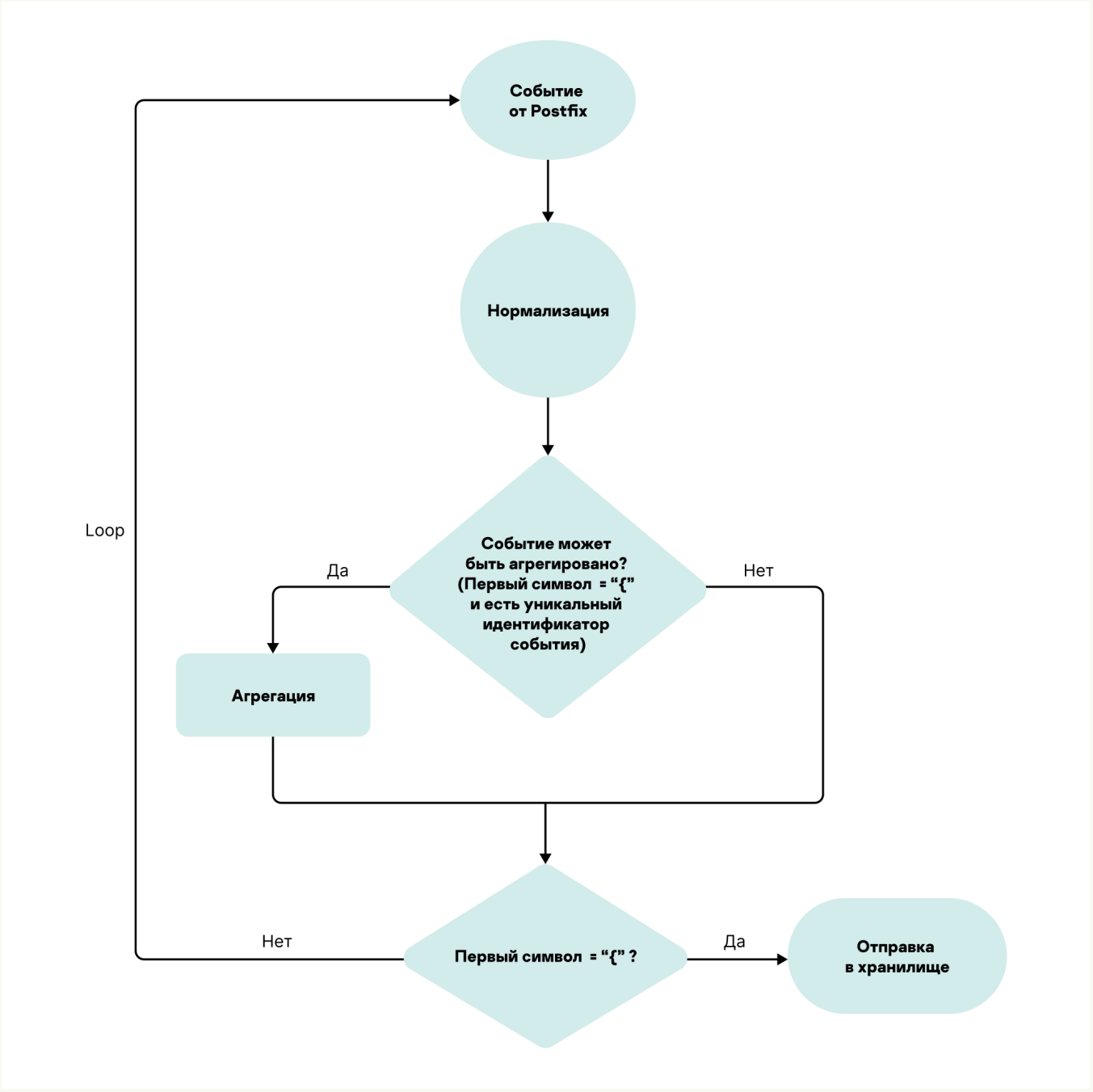


Схема обработки событий от системы Postfix

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 LogAnalyzer:

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 LogAnalyzer для получения и обработки событий Postfix

Чтобы настроить коллектор LogAnalyzer для получения событий Postfix:

1. Импортируйте пакет [OOTB] Postfix из репозитория LogAnalyzer. Пакет доступен для LogAnalyzer 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 две точки назначения: этот же коллектор с именем `Loop` и хранилище.

        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 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.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора создан с заданными параметрами в веб-интерфейсе LogAnalyzer. 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 LogAnalyzer. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP. Ресурсы, описанные в этой статье, доступны для LogAnalyzer 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 LogAnalyzer для получения событий CommuniGate Pro.

3. Проверка поступления событий CommuniGate Pro в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий CommuniGate Pro выполнена правильно в разделе веб-интерфейса LogAnalyzer 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 LogAnalyzer, 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 в хранилище будет направлено одно событие.

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.

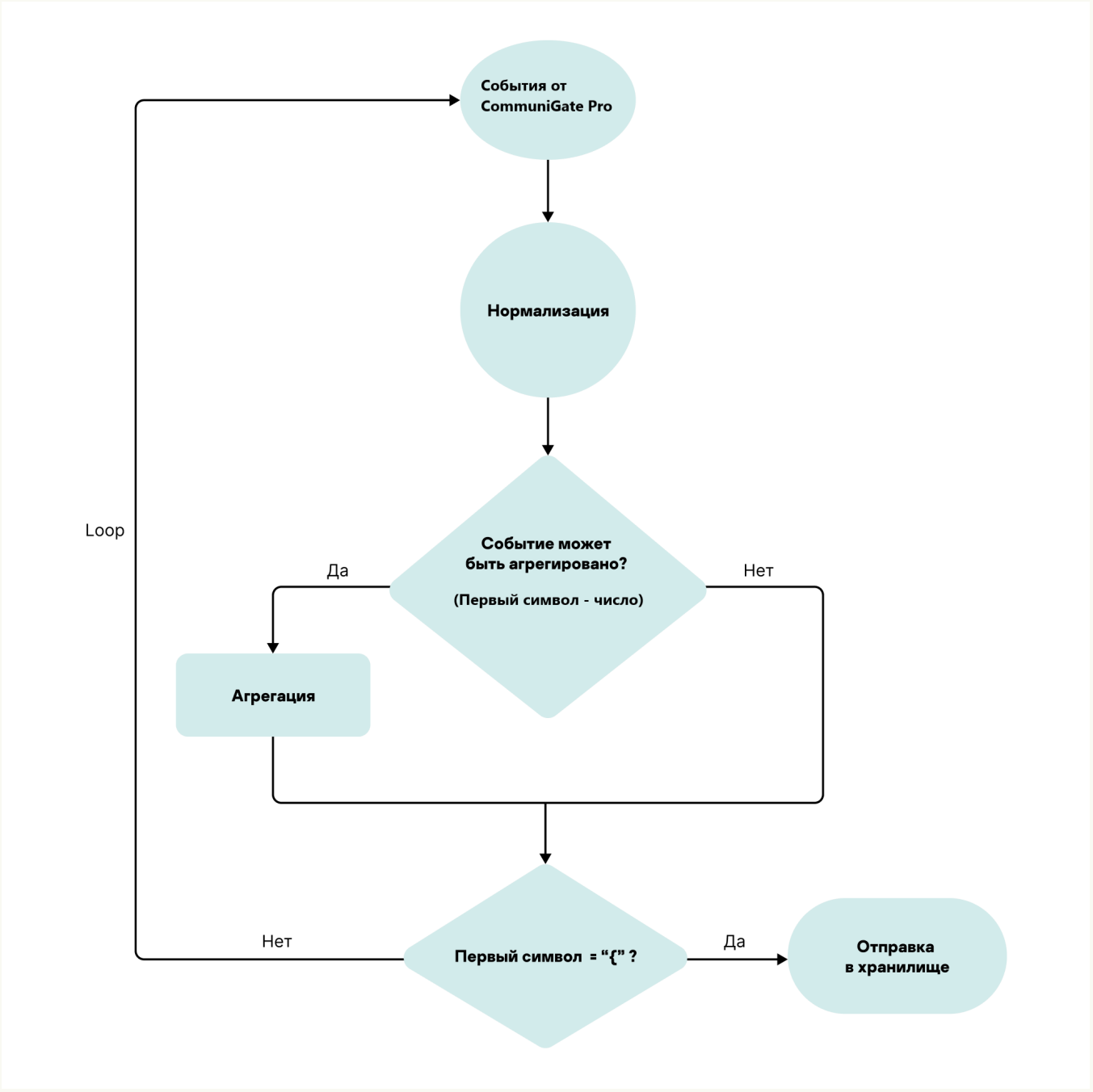


Схема обработки событий от системы CommuniGate Pro

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 LogAnalyzer необходимо установить на сервер CommuniGate Pro агент LogAnalyzer и настроить чтение файлов с расширением .log из директории /var/CommuniGate/SystemLogs/ и отправку по протоколу TCP в коллектор LogAnalyzer.

Чтобы создать агент, который будет выполнять чтение и передачу в LogAnalyzer событий:

1. В веб-консоли LogAnalyzer 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 LogAnalyzer.
4. Нажмите на кнопку **Создать**.
5. После того как сервис агента создан в LogAnalyzer, следует установить агент на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

Настройка коллектора LogAnalyzer для получения и обработки событий CommuniGate Pro

Чтобы настроить коллектор LogAnalyzer для получения событий CommuniGate Pro:

1. Импортируйте пакет [OOTB] CommuniGate Pro из репозитория LogAnalyzer. Пакет доступен для LogAnalyzer 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 две точки назначения: этот же коллектор с именем `Loop` и хранилище.

        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.

        a. 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.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора создан с заданными параметрами в веб-интерфейсе LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer для получения и обработки событий Yandex Cloud.

   Для получения событий Yandex Cloud в мастере установки коллектора LogAnalyzer необходимо выполнить следующие действия:

   1. В мастере установки коллектора LogAnalyzer 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 LogAnalyzer.
5. Проверка поступления событий Yandex Cloud в коллектор LogAnalyzer.

   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 LogAnalyzer.

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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка доступа к интерфейсам API управления Office 365 стандартными методами Microsoft

   Для получения событий в LogAnalyzer выдайте необходимый набор разрешений API:

   Microsoft.Graph

   Directory.Read.All

   API управления Office 365

   ActivityFeed.Read

   ActivityFeed.Read.Dlp

2. Создание коллектора LogAnalyzer

   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 LogAnalyzer

4. Проверка поступления событий Microsoft 365 в коллектор LogAnalyzer

   Чтобы проверить, что настройка сервера источника событий Microsoft 365 выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка получения событий АПКШ Континент

В поставку LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer состоит из следующих этапов:

1. Подготовительные действия для получения событий АПКШ Континент.

   На данном этапе необходимо создать коллектор LogAnalyzer, 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 LogAnalyzer. Доступен журнал kuma-kont.log.

Подготовительные действия для получения событий АПКШ Континент

1. Создание коллектора LogAnalyzer.

   1. Создание коллектора LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer.

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 LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer.

В случае использования протокола TCP для отправки событий при потере соединения с коллектором LogAnalyzer 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.

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.
`alert_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа AlertLog, с которого необходимо начать отправлять события в коллектор LogAnalyzer. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0

Параметр	Описание
`packet_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа PacketLog, с которого необходимо начать отправлять события в коллектор LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer.
`port`	Обязательный параметр в группе **KUMA Collector**. Порт коллектора LogAnalyzer.
`protocol`	Обязательный параметр в группе **KUMA Collector**. Протокол передачи данных, который используется в коллекторе LogAnalyzer. Если используется протокол udp, повторная отправка событий при потере соединения с коллектором LogAnalyzer не будет осуществлена. Доступные значения: • **tcp** • **udp**

Настройка получения событий VK WorkSpace Mail

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.
4. Проверка поступления событий VK WorkSpace Mail в коллектор LogAnalyzer.

   Вы можете проверить, что настройка сервера источника событий VK WorkSpace Mail выполнена правильно в разделе веб-интерфейса LogAnalyzer Поиск связанных событий.

Настройка отправки событий VK WorkSpace Mail

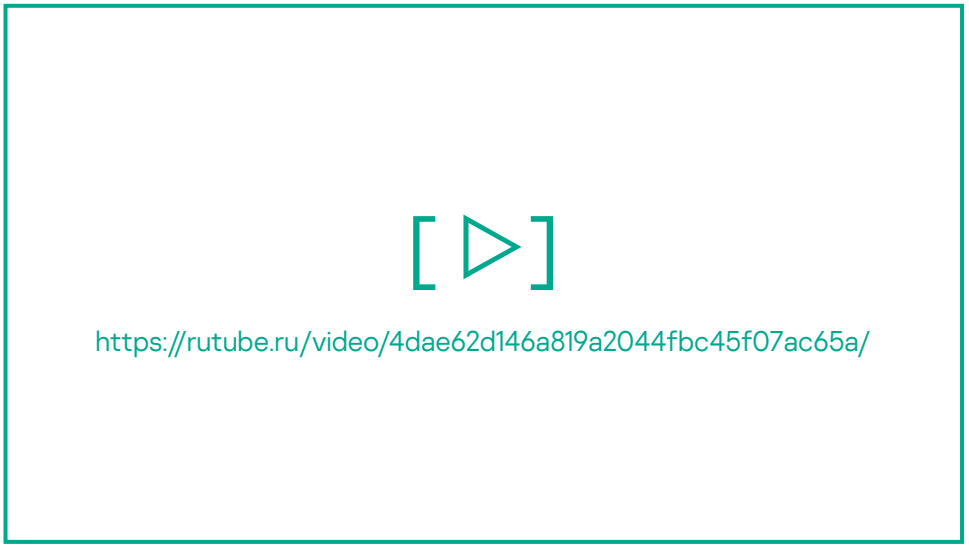
Для настройки передачи событий в LogAnalyzer выполните следующие действия:

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 LogAnalyzer.
   b. В поле **Порт сервера syslog** укажите порт, который прослушивает коллектор LogAnalyzer.
   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.

Мониторинг источников событий

В этом разделе представлена информация о мониторинге источников событий.



https://rutube.ru/video/4dae62d146a819a2044fbc45f07ac65a/

Состояние источников

В LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer начала определять источники с учетом новых параметров, перезапустите коллекторы.

Чтобы определить источники событий:

1. В веб-интерфейсе LogAnalyzer перейдите в раздел **Состояние источников**.

2. В открывшемся окне **Состояние источников** нажмите кнопку в виде гаечного ключа.

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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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**.

   LogAnalyzer 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 LogAnalyzer 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.

   LogAnalyzer выполнит обогащение и зарегистрирует источник событий.

2. Если в LogAnalyzer поступают события с одинаковыми значениями полей, определяющих источник, LogAnalyzer 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 LogAnalyzer регистрировала для таких событий один источник, вы можете дополнительно настроить поля в нормализаторе.

Списки источников формируются в коллекторах, объединяются в Ядре LogAnalyzer и отображаются в веб-интерфейсе программы 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 LogAnalyzer 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 на источник назначены политики мониторинга только типа **byCount** или политики мониторинга разных типов, отображается как количество событий. Если на источник назначены политики мониторинга только типа **byEPS** или политики не назначены, отображается как количество событий в секунду.

- **Тенант** – тенант, к которому относятся события, поступающие из источника.

Управление источниками событий

Вы можете выбрать один или несколько источников событий, установив флажки в первом столбце таблицы. Вы можете выбрать сразу несколько источников событий для выполнения групповых операций, установив флажок в первом столбце в заголовке таблицы и выбрав **Выбрать все** или **Выбрать все на странице**. Вариант **Выбрать все на странице** работает только с отображаемыми в списке источниками событий: если в списке отображаются только 500 из 1500 источников, то групповые действия по выгрузке, включению или 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 LogAnalyzer 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 LogAnalyzer 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.
   - **Выбрать все на странице** – выбрать все источники событий на открытой странице. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники на открытой странице, удовлетворяющие условию поиска.

2. Нажмите на кнопку **CSV** 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer с интервалом в 15 секунд собирает с коллекторов информацию о потоке.

3. Собранные данные хранятся на сервере Ядра LogAnalyzer в СУБД временных рядов Victoria Metrics, и глубина хранения данных на сервере Ядра LogAnalyzer 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 во все хранилища тенанта Main.

Добавление политики мониторинга

Чтобы добавить новую политику мониторинга:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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.

   - **Выбрать все на странице** – выбрать все источники событий, прогрузившиеся на открытой странице. Если вы отфильтровали источники с помощью поиска, будут выбраны все источники на открытой странице, удовлетворяющие условию поиска.

   В левой нижней части таблицы отображается количество выбранных источников и общее количество источников в таблице.

   После того как вы выберете в списке источники событий, к которым хотите применить политику мониторинга, 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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.

Интеграция с другими решениями

В этом разделе описано, как интегрировать LogAnalyzer с другими приложениями для расширения возможностей программы.

Интеграция с Kaspersky CyberTrace

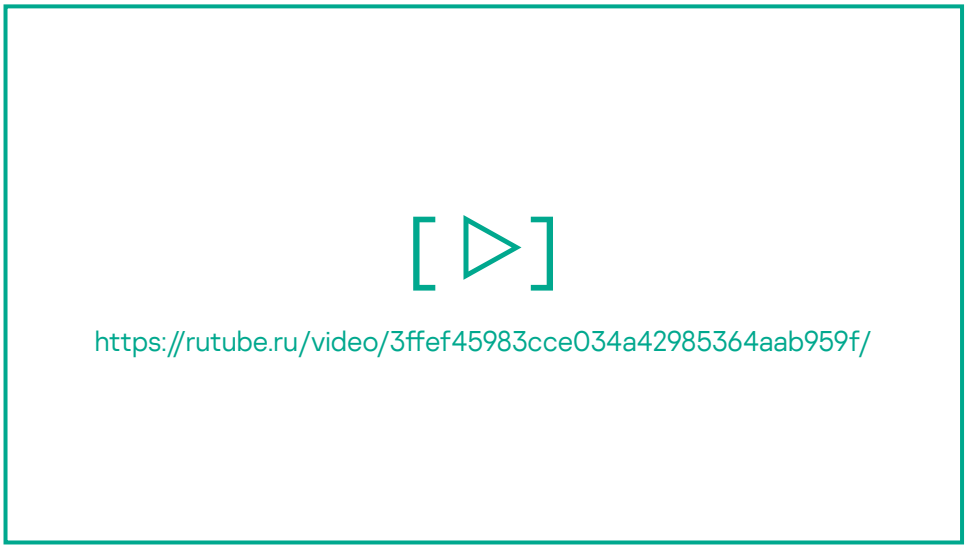
Kaspersky CyberTrace (далее CyberTrace) – это инструмент, который объединяет потоки данных об угрозах с решениями SIEM. Он обеспечивает пользователям мгновенный доступ к данным аналитики, повышая их осведомленность при принятии решений, связанных с безопасностью.

Вы можете интегрировать CyberTrace с LogAnalyzer одним из следующих способов:

- Интегрировать функцию поиска индикаторов CyberTrace для обогащения событий LogAnalyzer информацией потоков данных CyberTrace.
- Интегрировать в LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

   Вы можете настроить интеграцию с LogAnalyzer сразу после установки CyberTrace в мастере первоначальной настройки или позднее в веб-интерфейсе CyberTrace.

2. Создать правила обогащения событий в LogAnalyzer.

   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 LogAnalyzer будут обогащаться данными из CyberTrace.

Пример проверки обогащения данными из CyberTrace.

По умолчанию проверка соединения с CyberTrace в LogAnalyzer 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 LogAnalyzer: 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer **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 LogAnalyzer. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро LogAnalyzer.

   h. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять LogAnalyzer в секунду. Значение по умолчанию: `1000`.

   i. В поле **Время ожидания** укажите время в секундах, в течение которого LogAnalyzer должна ожидать ответа от сервера CyberTrace. 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 LogAnalyzer, 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 раскарывающемся 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

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.
- **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 LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer. Когда эта интеграция включена, в веб-интерфейсе LogAnalyzer появляется раздел **CyberTrace** с доступом к веб-интерфейсу CyberTrace. Вы можете настроить интеграцию в разделе **Интеграции** → **Kaspersky CyberTrace** веб-интерфейса LogAnalyzer.

Чтобы интегрировать веб-интерфейс CyberTrace в LogAnalyzer:

1. Откройте раздел веб-интерфейса LogAnalyzer **Ресурсы** → **Конфигурация ресурсов** → **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 LogAnalyzer.

5. Откройте раздел веб-интерфейс LogAnalyzer **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 LogAnalyzer.
   - **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 LogAnalyzer.

     Для этого в разделе Разрешить хосты нажмите Добавить хост и в появившемся поле укажите IP или hostname устройства,

     на котором развернут веб-интерфейс LogAnalyzer.

   - Использовать FQDN при входе в веб-интерфейс LogAnalyzer.

     Если для работы в веб-интерфейсе программы 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 LogAnalyzer: раздел **CyberTrace** отображается в веб-интерфейсе LogAnalyzer.

*Чтобы настроить отображение данных в разделе **CyberTrace** при использовании FQDN для входа в LogAnalyzer в Mozilla Firefox:*

1. Очистите кеш браузера.

2. В строке браузера введите FQDN веб-интерфейса LogAnalyzer 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 LogAnalyzer будет создано исключение.

5. В строке браузера введите URL-адрес веб-интерфейса LogAnalyzer 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 LogAnalyzer, можно обновлять список запрещенных объектов CyberTrace или **Internal TI** данными из событий LogAnalyzer.

Чтобы обновить Internal TI в CyberTrace:

1. Откройте область деталей события в таблице событий 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 LogAnalyzer, нажмите **Да**.

Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

Настройка обогащения событий и ретроспективного сканирования

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Интеграция LogAnalyzer с Kaspersky CyberTrace (далее CyberTrace) версии 5.0 и выше позволяет обогащать события информацией об индикаторах компрометации (IoC) и выполнять ретроспективное сканирование (ретроспективную проверку) 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, если вы хотите перепроверить сохраненные события на наличие новых угроз.

Чтобы настроить обогащение данных и ретроспективное сканирование:

1. Выполните первоначальную настройку в LogAnalyzer, 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 ретроспективной проверки.

   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 LogAnalyzer.

   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 LogAnalyzer.

   Пример оповещения:

   ```
   Category=KUMA_Demo_1_Hash_SHA1|MatchedIndicator=E1B85D995DC09DE25603D0B7A67D998015F6C045|
   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_repo
   C2DF-4AED-B430-2E64AEF781FC
   ```

Интеграция с Kaspersky Threat Intelligence Portal

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Портал Kaspersky Threat Intelligence Portal объединяет все знания "Лаборатории Касперского" о киберугрозах и их взаимосвязи в единую веб-службу. При интеграции с LogAnalyzer портал помогает пользователям LogAnalyzer 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

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Чтобы интегрировать Kaspersky Threat Intelligence Portal в LogAnalyzer:

1. Откройте раздел веб-интерфейса LogAnalyzer **Ресурсы**.
2. В блоке **Конфигурация ресурсов** 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 LogAnalyzer.
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 из Kaspersky Threat Intelligence Portal в LogAnalyzer после завершения интеграции.

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 LogAnalyzer завершен.

После интеграции Kaspersky Threat Intelligence Portal и LogAnalyzer 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

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий 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.

Просмотр данных от Kaspersky Threat Intelligence Portal

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Чтобы просмотреть данные из Kaspersky Threat Intelligence Portal,

Откройте область деталей события в таблице событий 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 LogAnalyzer 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

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Чтобы обновить данные, полученные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий 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 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.

Аутентификация с помощью доменных учетных записей

Чтобы пользователи могли проходить аутентификацию в веб-интерфейсе LogAnalyzer 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 LogAnalyzer группу домена. Пользователи из этой группы, пройдя аутентификацию с помощью своих доменных учетных данных, будут получать доступ к веб-интерфейсу LogAnalyzer в соответствии с указанной ролью.

При этом программа проверяет соответствие группы пользователя указанному фильтру в порядке следования ролей в веб-интерфейсе LogAnalyzer: 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.

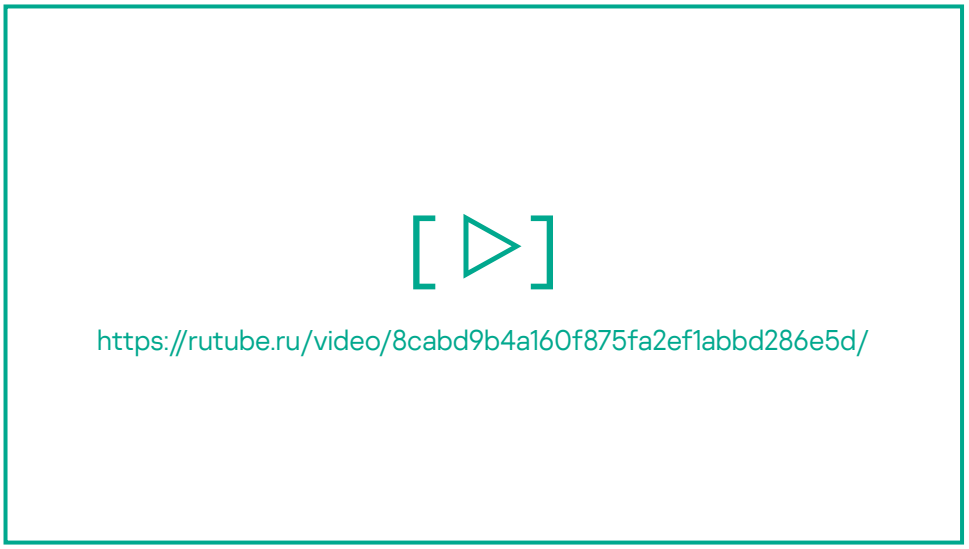
Особенности входа в систему после настройки доменной аутентификации

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 LogAnalyzer 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 LogAnalyzer не будет создана.
- Локальная учетная запись LogAnalyzer 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 LogAnalyzer.
- 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 отключить ее в веб-интерфейсе LogAnalyzer, не удаляя заданные ранее значения параметров. При необходимости вы сможете в любой момент включить аутентификация снова.

Чтобы включить или отключить доменную авторизацию пользователей в веб-интерфейсе LogAnalyzer:

1. В веб-интерфейсе программы 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 настройки 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 программы 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 LogAnalyzer будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа 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 LogAnalyzer, в поле **Группа главных администраторов** укажите DistinguishedName группы FreeIPA, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в LogAnalyzer 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 программы 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 LogAnalyzer.

> 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 программы 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer.

Настройка соединения LogAnalyzer 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 программы 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 LogAnalyzer будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа 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 LogAnalyzer, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в LogAnalyzer 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 программы 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 LogAnalyzer.

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 программы 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer.

Настройка соединения LogAnalyzer с Active Directory Federation Services

Чтобы настроить доменную аутентификацию в LogAnalyzer 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 LogAnalyzer 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 программы 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory Federation Services, в которой состоит пользователь. Для Главного администратора дополнительные роли активированы в LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

> 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 программы 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer.

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 (ADFS).

На сервере должна быть уже настроена роль ADFS.

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 ADFS 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 опций **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 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 ADFS 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 выполнит переход 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 ADFS завершена. Вы можете переходить к настройке доменной аутентификации в KUMA.

Устранение ошибки Access denied

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 NeuroDAT SIEM IM

Система NeuroDAT SIEM IM предназначена для мониторинга информационной безопасности.

Вы можете настроить передачу событий LogAnalyzer в NeuroDAT SIEM IM. На основе поступающих событий в системе NeuroDAT SIEM IM автоматически формируются инциденты информационной безопасности.

Чтобы настроить интеграцию с NeuroDAT SIEM IM:

1. Подключитесь к серверу NeuroDAT SIEM IM по протоколу SSH под учётной записью с административными привилегиями.

2. Создайте резервную копию конфигурационного файла /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties.

3. В конфигурационном файле /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties установите указанные значения для следующих параметров:

   - `kuma.on=true`

     Этот параметр является признаком взаимодействия с NeuroDAT SIEM IM с LogAnalyzer.

   - `job_kuma=com.cbi.soz.server.utils.scheduler.KumaIncidentsJob`

   - `jobDelay_kuma=5000`

   - `jobPeriod_kuma=60000`

4. Сохраните изменения конфигурационного файла.

5. Перезапустите сервис tomcat с помощью команды:

   ```
   sudo systemctl restart tomcat
   ```

6. Получите токен для пользователя в LogAnalyzer. Для этого выполните следующие действия:

   a. Откройте веб-интерфейс LogAnalyzer, 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.

   b. Нажмите на кнопку **Сгенерировать токен**.

      Откроется окно **Новый токен**.

   c. 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.

   d. Нажмите на кнопку **Сгенерировать токен**.

      В области деталей пользователя отобразится поле **Токен** с автоматически созданным токеном. Скопируйте его.

      При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

   e. Нажмите **Сохранить**.

7. Войдите в NeuroDAT SIEM IM под учетной записью admin или другой учётной записью, обладающей ролью Администратор для настраиваемой организации или Администратор всех организаций.

8. В пункте меню **Администрирование** → **Структура организации** выберите или создайте организацию, которая будет получать инциденты из LogAnalyzer.

9. На форме организации выполните следующие действия:

   a. Установите флажок **Настроить интеграцию с KUMA**.

   b. В поле **IP адрес и сетевой порт KUMA** укажите адрес API LogAnalyzer, например `https://192.168.58.27:7223/api/v1/`.

   c. В поле **Ключ API KUMA** укажите токен пользователя, полученный на шаге 6.

   d. Сохраните данные организации.

Настройка интеграции с LogAnalyzer будет завершена.

NeuroDAT SIEM IM выполнит проверку доступа к LogAnalyzer и в случае успеха отобразит сообщение о готовности получать данные из LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer и сделайте файл утилиты исполняемым при помощи команды:

   ```
   chmod +x <путь до файла redcheck-tool.py>
   ```

5. Запустите утилиту redcheck-tool.py с помощью следующей команды:

   ```
   python3 redcheck-tool.py --kuma-rest <адрес и порт сервера KUMA REST API> --token <API-токен> --tenant <название тенанта, куда будут помещены активы> --vuln-report <полный путь к файлу отчета "Уязвимости"> --inventory-report <полный путь к файлу отчета "Инвентаризация">
   ```

   Пример:
   ```
   python3 --kuma-rest example.kuma.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report /home/user/vuln.csv --inventory-report /home/user/inventory.csv
   ```

   Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения расширенного отчета о полученных активах `-v`. Подробное описание доступных флагов и команд приведено в таблице "Флаги и команды утилиты redcheck-tool.py". Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета RedCheck в LogAnalyzer. 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:

- LogAnalyzer перезаписывает данные импортированных через API активов и удаляет сведения об их устраненных уязвимостях.
- LogAnalyzer пропускает активы с недействительными данными.

Флаги и команды утилиты redcheck-tool.py

Флаги и команды	Обязательный	Описание
`--kuma-rest < адрес и порт сервера LogAnalyzer >`	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 LogAnalyzer, 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 LogAnalyzer.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования Sendmail.
2. Настройка сервера источника событий.
3. Создание коллектора LogAnalyzer.

   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 LogAnalyzer.
5. Проверка поступления событий Sendmail в коллектор LogAnalyzer.

   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 LogAnalyzer 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 @<<IP-адрес коллектора>:<порт коллектора>>
   ```

   Пример:

   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'sendmail' then @@<<IP-адрес коллектора>:<порт коллектора>>
   ```

3. Создайте резервную копию файла /etc/rsyslog.conf.
4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения.
6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Управление LogAnalyzer

В этом разделе описываются общие параметры LogAnalyzer.

Вход в веб-интерфейс приложения

В веб-интерфейс LogAnalyzer могут входить только пользователи со статусом учетных записей *Активная*.

Рекомендуем настроить требования к паролям и правила входа в веб-интерфейс приложения в политике безопасности.

Чтобы войти в веб-интерфейс приложения:

1. В браузере введите следующий адрес:

   ```
   https://<IP-адрес или FQDN сервера Ядра LogAnalyzer>: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.

4. Нажмите на кнопку **Логин**.

   Если вы ввели неверные учетные данные, LogAnalyzer сможет обработать следующую попытку входа через 3 секунды. Задержка по времени помогает предотвратить вход злоумышленника в веб-интерфейс LogAnalyzer с помощью перебора пароля. Если вы введете неверные учетные данные несколько раз подряд, ваша учетная запись заблокируется. Максимальное количество неудачных попыток входа и длительность блокировки учетной записи регулируются политикой безопасности.

Откроется главное окно веб-интерфейса приложения.

В режиме мультитенантности при первом входе в веб-интерфейс приложения пользователю отображаются данные только для тех тенантов, которые были выбраны для него при создании его учетной записи.

Чтобы выйти из веб-интерфейса приложения,

откройте веб-интерфейс LogAnalyzer, в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Выход**.

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 LogAnalyzer и если заданные пороговые значения будут превышены, произойдут следующие изменения:

  - LogAnalyzer зарегистрирует событие аудита Зарегистрирован алерт Victoria Metrics для сервиса.
  - LogAnalyzer 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 LogAnalyzer **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 LogAnalyzer **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 LogAnalyzer перейдите в раздел **Параметры** → **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 LogAnalyzer регистрирует аудит событие Пороговые значение параметров мониторинга сервисов изменены.

LogAnalyzer 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 LogAnalyzer перейдите в раздел **Параметры** → **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 LogAnalyzer будет отключен, при этом сервисам не будет присваиваться желтый статус.

Просмотр метрик LogAnalyzer

Для отслеживания работы своих компонентов , потока событий в LogAnalyzer выполняется сбор и хранение большого количества параметров. Для сбора, хранения и анализа параметров используется решение VictoriaMetrics, представляющее собой СУБД в формате временных рядов. Визуализация собранных метрик осуществляется с помощью Grafana. В разделе LogAnalyzer → **Метрики** представлены панели мониторинга с визуализацией ключевых параметров работы различных компонентов LogAnalyzer.
Сервис Ядра LogAnalyzer выполняет настройку параметров VictoriaMetrics и Grafana автоматически, участие пользователя не требуется.

Визуализация собранных метрик осуществляется с помощью решения Grafana. RPM-пакет службы kuma-core формирует конфигурацию Grafana и создает отдельную панель мониторинга для визуализации метрик каждого сервиса. Графики в разделе **Метрики** появляются с задержкой около 1,5 минут.

Полная информация о метриках доступна в разделе **Метрики** веб-интерфейса LogAnalyzer. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра. Если в разделе **Метрики** вы видите core:<номер порта>, это означает, что LogAnalyzer развернута в отказоустойчивой конфигурации и метрики получены с хоста, на котором было **установлено Ядро LogAnalyzer**. В прочих конфигурациях отображается имя хоста, с которого LogAnalyzer 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
```

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

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

Метрики коллекторов

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных за секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения за 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 за 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 за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size (размер дискового буфера)	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 за секунду.
Connector errors (ошибки коннектора)	Количество ошибок в логах коннектора.

Normalization (нормализация) – метрики, относящиеся к нормализаторам.	
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.	
EPS (события, обрабатываемые за секунду)	Количество событий, удовлетворяющих условиям фильтра и отправленных в обработку за секунду. Коллектор обрабатывает события, удовлетворяющие условиям фильтра, только если пользователь добавил фильтр в конфигурацию сервиса коллектора.

Aggregation (агрегация) – показатели, относящиеся к правилам агрегации.	
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.	
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.

Метрики корреляторов

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных за секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения за 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 за 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 за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size (размер дискового буфера)	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.

Correlation (корреляция) – метрики, относящиеся к правилам корреляции.	
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.

Enrichment (обогащение) – метрики, относящиеся к правилам обогащения.	
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.	
RPS (запросы в секунду)	Количество активаций правила реагирования за секунду.

Метрики хранилища

Название метрики	Описание
Storage / IO (ввод-вывод) – метрики, относящиеся к состоянию узлов кластера ClickHouse.	
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.	
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 за секунду.
Failed QPS (безуспешные запросы в секунду)	Количество безуспешных запросов, отправленных кластеру ClickHouse за секунду.
Allocated memory (назначенная память)	Количество RAM в гигабайтах, назначенное процессу ClickHouse.

ClickHouse / Insert (вставка) – метрики, относящиеся к вставке событий в экземпляр ClickHouse.	
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.	
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.	
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.	
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.

Метрики Ядра LogAnalyzer

Название метрики	Описание
Raft – метрики, относящиеся к чтению и обновлению состояния Ядра LogAnalyzer.	
Lookup RPS (запросы на чтение в секунду)	Количество запросов на выполнение процедур чтения, отправленных Ядру LogAnalyzer 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.
Propose RPS (запросы на обновление состояния в секунду)	Количество запросов на выполнение процедур обновления состояния Raft (SQLite), отправленных Ядру LogAnalyzer 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.
Tasks – метрики, относящиеся к мониторингу выполнения задач на Ядре LogAnalyzer	
Active tasks	Количество выполняемых задач за единицу времени.

Название метрики	Описание
Task Execution latency	Время выполняемых задач в секундах.
Errors	Количество ошибок при выполнении задач.

API – метрики, относящиеся к API-запросам.	
RPS (запросы в секунду)	Количество API-запросов, отправленных Ядру LogAnalyzer за секунду.
Latency (задержка)	Время в миллисекундах, затраченное на обработку одного API-запроса к Ядру LogAnalyzer. Отображается медиана.
Errors (ошибки)	Количество ошибок, возникших за секунду при отправке API-запросов Ядру LogAnalyzer.

Notification Feed (фид уведомлений) – метрики, относящиеся к активности пользователей.	
Subscriptions (подписки)	Количество клиентов, подключенных к Ядру LogAnalyzer через SSE для получения сообщений сервера в реальном времени. Обычно это число равно количеству клиентов, использующих веб-интерфейс LogAnalyzer.
Errors (ошибки)	Количество ошибок, возникших за секунду при отправке уведомлений пользователям.

Schedulers (планировщики) – метрики, относящиеся к задачам Ядра LogAnalyzer.	
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 за секунду при выполнении задач.

Метрики агента LogAnalyzer

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных за секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения за 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 за 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 за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size (размер дискового буфера)	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 за секунду.

Метрики Event routers

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS (обрабатываемые события в секунду)	Количество событий, обработанных за секунду.
Output EPS (вывод событий)	Количество событий, отправленных точке назначения за 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 за 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 за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size (размер дискового буфера)	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 за секунду.
Connector Errors (ошибки коннектора)	Количество ошибок в журнале коннектора.

Метрики, общие для всех сервисов

Название метрики	Описание
Process – общие метрики процесса.	
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 (ОС) – метрики, относящиеся к операционной системе.	
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.

Срок хранения метрик

По умолчанию данные о работе LogAnalyzer хранятся 3 месяца. Этот срок можно изменить.

Чтобы изменить срок хранения метрик LogAnalyzer:

1. Войдите в ОС сервера, на котором установлено Ядро LogAnalyzer.
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 LogAnalyzer, выполнив последовательно следующие команды:
   a. `systemctl daemon-reload`
   b. `systemctl restart kuma-victoria-metrics`

Срок хранения метрик изменен.

Работа с задачами LogAnalyzer

При работе в веб-интерфейсе программы вы можете выполнять различные операции с помощью задач. Например, вы можете выполнить импорт активов или экспортировать информацию о событиях LogAnalyzer 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 программы.

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.
  - **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 программе доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий LogAnalyzer.
  - **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 LogAnalyzer с помощью Kaspersky Endpoint Detection and Reponse.
  - **Обновление репозитория** – обновления репозитория LogAnalyzer 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.
- **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 программы. 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 LogAnalyzer 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 LogAnalyzer 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.

   - 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.

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в разделе веб-интерфейса LogAnalyzer **Параметры** → **Другое** → **Общие** → **Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. Откройте веб-интерфейс LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer.

Уведомления LogAnalyzer

Уведомления в веб-интерфейсе LogAnalyzer

По умолчанию для всех пользователей установлен флажок **Уведомлять об алертах в веб-интерфейсе** и в веб-интерфейсе LogAnalyzer отображаются уведомления об алертах.

При необходимости отображение таких уведомлений можно выключить, сняв флажок в профиле пользователя.

Стандартные уведомления

В LogAnalyzer 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 LogAnalyzer. После каждого перезапуска Ядра отсчет 6-часового интервала начинается заново.

LogAnalyzer автоматически уведомляет пользователей о следующих событиях:

- создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета);
- выполнена задача (уведомление получают пользователи, создавшие задачу).
- доступны новые пакеты с ресурсами, которые можно получить путем обновления репозитория LogAnalyzer (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи).
- превышено среднесуточное количество EPS, ограниченное лицензией.
- превышено среднечасовое количество EPS, ограниченное лицензией SMB.

Журналы LogAnalyzer

В LogAnalyzer 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

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer>/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 LogAnalyzer в разделе **Параметры** → **Другое** → **Общие** → **Параметры Ядра** → **Отладка**. Где хранятся: /opt/kaspersky/kuma/core/<идентификатор сервиса Ядра LogAnalyzer>/log/core Журналы Ядра можно скачать в веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы**, выбрав сервис Ядра и нажав на кнопку **Журнал**. Если LogAnalyzer установлена в отказоустойчивой конфигурации, см. ниже раздел *Просмотр журналов Ядра в Kubernetes*.

Сервисы:
• Хранилище
• Коллекторы
• Агенты
	Как включить: в параметрах сервиса с помощью переключателя **Отладка**.
	
	Где хранятся: в директории установки сервиса. Например, /opt/kaspersky/kuma/<тип сервиса collector/storage>/<идентификатор сервиса>/log/<тип сервиса collector/storage>. Журналы сервисов можно скачать в веб-интерфейсе LogAnalyzer в разделе **Ресурсы** → **Активные сервисы**, выбрав нужный сервис и нажав на кнопку **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 >`
	
	• 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 LogAnalyzer, 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer будет использовано значение 0.	`56.835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в LogAnalyzer будет использовано значение 0.	`60.612778`

Конвертация геоданных из MaxMind и IP2Location

В LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer>
--input <путь к ZIP-архиву с геоданными из MaxMind или IP2location>
```

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта:
`python converter.py --help`

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out
geoip_maxmind_ru.csv
```

Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла GeoLite2-City-Locations-en.csv из ZIP-архива.

Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out
geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP
IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out geoip_ip2location_ipv4_ipv6.csv
```

Параметр `--lang` для IP2Location не используется.

Обязательные наборы полей

Исходные файлы MaxMind GeoLite2-City-Blocks-IPv4.csv и GeoLite2-City-Blocks-IPv6.csv должны содержать следующий набор полей:

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

Пример набора исходных данных:

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000

1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

Остальные файлы CSV с кодом локали должны содержать следующий набор полей:

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union
```

Пример набора исходных данных:

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0

7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

Исходные файлы IP2Location должны содержать данные о диапазонах сетей, Country, Region, City, Latitude, Longitude

Пример набора исходных данных:

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"

"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"

"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+0
```

Если исходные файлы будут содержать другой набор полей, отличный от указанного в этом разделе, или каких-то полей будет не хватать, после конвертации отсутствующие поля в итоговом файле CSV будут пустыми.

Импорт и экспорт геоданных

При необходимости в LogAnalyzer 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 LogAnalyzer создается событие аудита.

Чтобы импортировать геоданные в LogAnalyzer:

1. Подготовьте CSV-файл с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать в поддерживаемый LogAnalyzer формат.

2. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer.

Чтобы экспортировать геоданные из LogAnalyzer,

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

Ресурсы LogAnalyzer

Ресурсы – это компоненты LogAnalyzer, 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 LogAnalyzer.

Ресурсы содержатся в разделе веб-интерфейса LogAnalyzer **Ресурсы** в блоке **Ресурсы**. Доступные типы ресурсов:

- **Нормализаторы** – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в LogAnalyzer. После обработки в нормализаторе сырое событие становится нормализованным и может обрабатываться другими ресурсами и сервисами LogAnalyzer.
- **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.
- **Словари** – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и сервисам LogAnalyzer.
- **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 LogAnalyzer 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**, **Фильтры**, **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.

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 LogAnalyzer 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 LogAnalyzer: 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 LogAnalyzer 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.

> Программа 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 уникальное имя ресурса в поле **Название**.

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, 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 LogAnalyzer 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 программа 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, программа 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).

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 её 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 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 её содержимому.

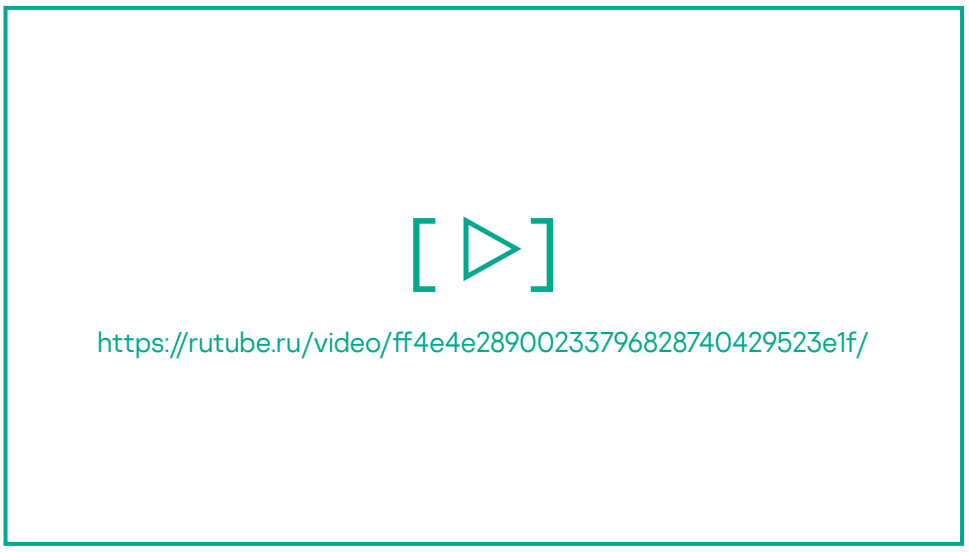
3. При необходимости в поле **Прокси-сервер** выберите из списка существующий прокси-сервер, который должен использоваться при запуске задачи **Обновление репозитория**.

   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 LogAnalyzer версии 4.0:

   - Выберите **Список программ**, затем нажмите на кнопку **Выбрать**. В открывшемся окне в разделе **Контроль периметра** установите флажок рядом с LogAnalyzer 4.0, 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_0=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 LogAnalyzer 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 LogAnalyzer 3.4 рекомендуется использовать ресурсы из пакета [OOTB] KUMA 3.4 resources и ресурсы, опубликованные в репозитории после выхода этого пакета.

LogAnalyzer поддерживает импорт ресурсов из более ранней версии в более позднюю, например из LogAnalyzer 3.4 в LogAnalyzer 4.0. Импорт из более поздней версии в более раннюю версию возможен, но не рекомендуется. Работоспособность такого ресурса не гарантируется.

Чтобы импортировать ресурсы:

1. В разделе **Ресурсы** нажмите **Импорт ресурсов**.

   Откроется окно **Импорт ресурсов**.

2. В раскрывающемся списке **Тенант** выберите тенанта, 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 LogAnalyzer. Ресурсы секретов импортируются пустыми.

Импорт ресурсов, использующих расширенную схему событий

Если вы импортируете нормализатор, использующий одно или несколько полей расширенной схемы событий, в LogAnalyzer 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 LogAnalyzer будет импортирован нормализатор, использующий поле расширенной схемы событий и такое поле уже существует в LogAnalyzer, будет использовано созданное ранее поле.

Если в LogAnalyzer будет импортирован нормализатор, использующий поле расширенной схемы событий, не соответствующее требованиям LogAnalyzer, 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 LogAnalyzer из файла, программа 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 LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer. 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. 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 LogAnalyzer 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 и тегам.

   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. LogAnalyzer выполняет поиск по JSON ресурса, если в нем указан другой ресурс, выполняет поиск по указанному ресурсу тоже. Если ресурс ссылается на другие ресурсы, LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer важно понимать, как одни ресурсы влияют на работоспособность других ресурсов, какие связи есть между ресурсами и другими объектами LogAnalyzer. Эти взаимозависимости вы можете отобразить визуально на интерактивном графе в веб-интерфейсе LogAnalyzer.

Отображение связей ресурса на графе

Чтобы отобразить связи выбранного ресурса:

1. В веб-консоли LogAnalyzer 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 агрегации;
- правила обогащения;
- 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;
- словари (доступно только в коммерческой версии LogAnalyzer);

- прокси-серверы;
- секреты;
- коллекторы;

  Особенность отображения связей: если для отображения связей был выбран, первично, коллектор, то связи "вверх" показываться не будут.

- 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**.

- 

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 , 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.

- 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

LogAnalyzer 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 LogAnalyzer, сравнивать версии, а также восстановить предыдущую версию ресурса, например, если необходимо восстановить его работоспособность.

Чтобы просмотреть историю изменений ресурса:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 для описания того, куда передавать обработанные события. Как правило, в роли точки назначения выступает 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 (доступно только в коммерческой версии LogAnalyzer) – используются для приема данных от сервисов LogAnalyzer по протоколу internal.
- storage – используются для передачи данных в хранилище.
- eventRouter (доступно только в коммерческой версии LogAnalyzer) – используются для передачи событий в маршрутизатор событий.

В поставку LogAnalyzer включена предустановленная точка назначения **[OOTB] Storage**, которая отправляет события в хранилище.

Точка назначения, тип internal

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Точки назначения с типом **internal** используются для приема данных от сервисов LogAnalyzer по протоколу internal. Вы можете передавать следующие данные по протоколу internal:

- Внутренние данные, такие как маршруты событий.
- Файловые атрибуты. Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом file, 1c-xml или 1c-log, на шаге Парсинг событий в таблице **Сопоставление** вы можете передать в поле события LogAnalyzer название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:
  - `$kuma_fileSourceName` – передать в поле события LogAnalyzer название обрабатываемого коллектором файла.
  - `$kuma_fileSourcePath` – передать в поле события LogAnalyzer путь к обрабатываемому коллектором файлу.

  Когда вы используете коннектор с типом **file**, **1c-xml** или **1c-log**, 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.

Параметр	Описание
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **internal**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `< имя хоста >:< номер порта >`; • `< IPv4-адрес >:< номер порта >`; • `< IPv6-адрес >< номер порта >`. IPv6-адреса можно указать в формате `[< IPv6-адрес >%< интерфейс >:< номер порта >`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. LogAnalyzer 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.
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.
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 ✎.
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
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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?**

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	• **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. • **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 .

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.
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. LogAnalyzer не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша ✎.

Параметр	Описание
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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?**

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	• **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. • **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 .

Точка назначения, тип eventRouter

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

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.
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. LogAnalyzer 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.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша ✎.

Параметр	Описание
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
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?**

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	• **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. • **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 .

Нормализаторы

Нормализаторы предназначены для приведения исходных событий, которые поступают из разных источников в разных форматах, к модели данных событий LogAnalyzer. Нормализованные события становятся доступны для обработки другими ресурсами и сервисами LogAnalyzer.

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 LogAnalyzer:

   - 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 LogAnalyzer 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.

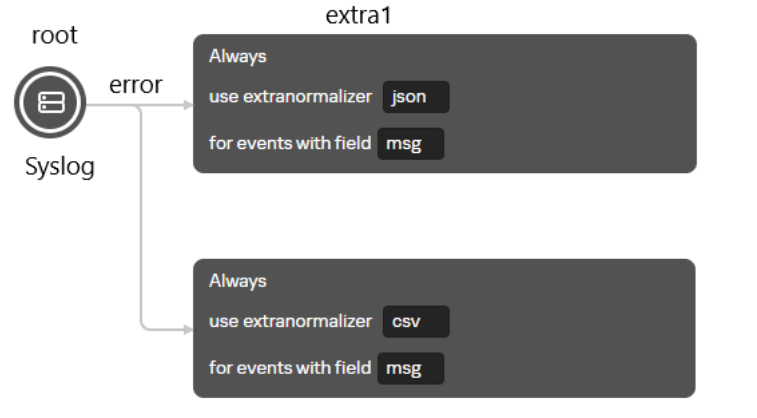
2. LogAnalyzer создает запись об ошибке в журнале коллектора.

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**.

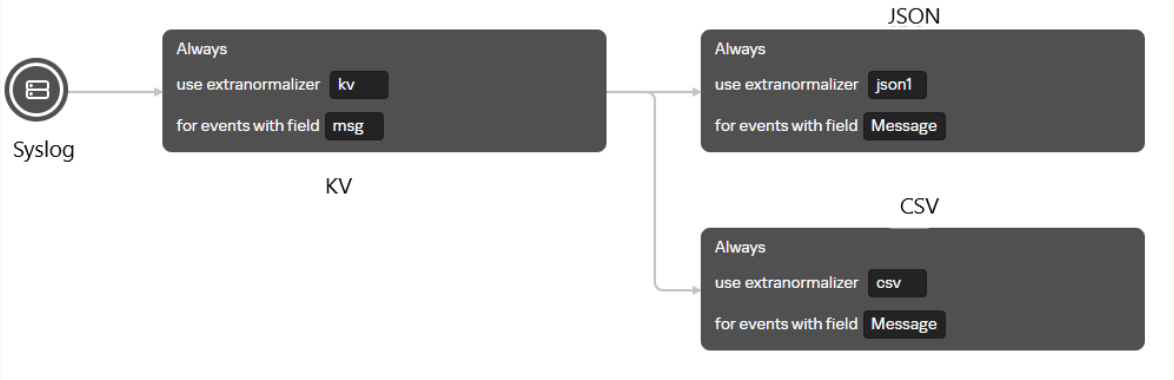


Схема нормализации событий

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**.

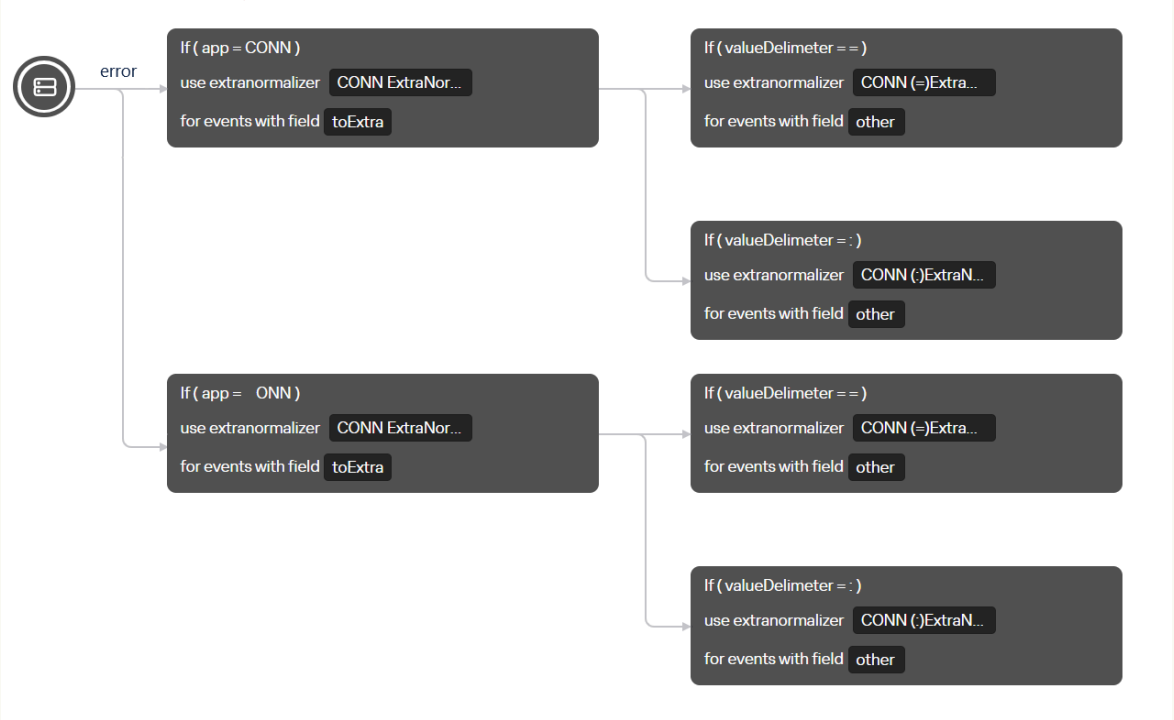


Схема возникновения ошибки

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**.

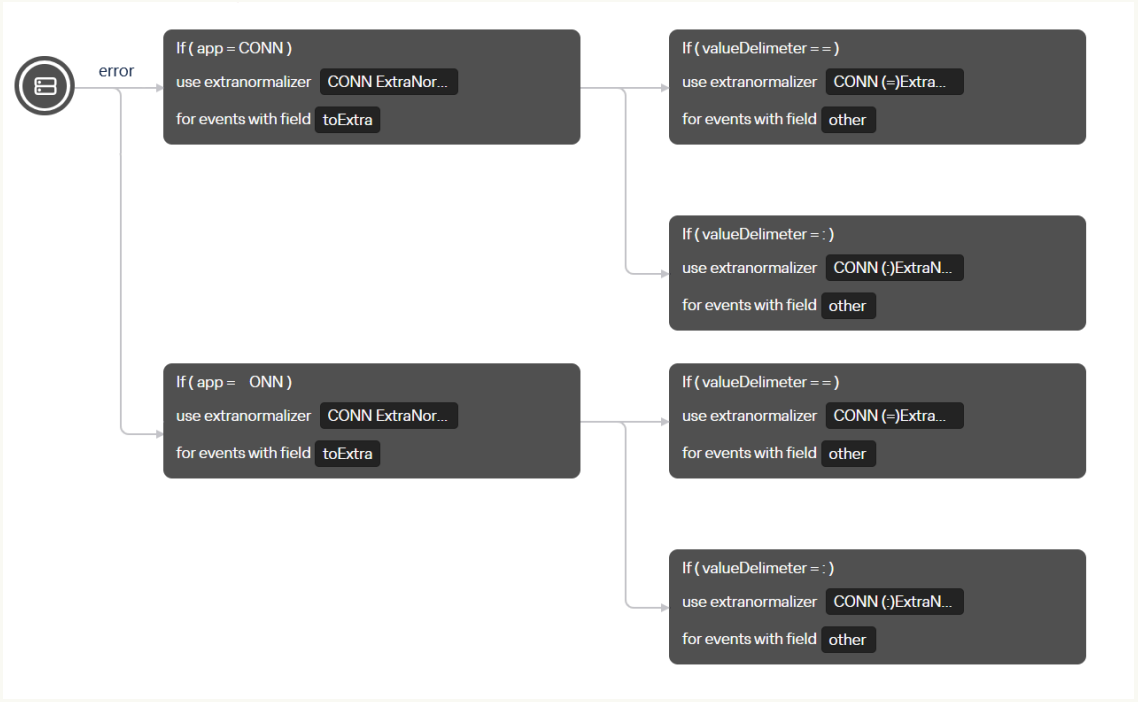


Схема возникновения ошибки

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**.

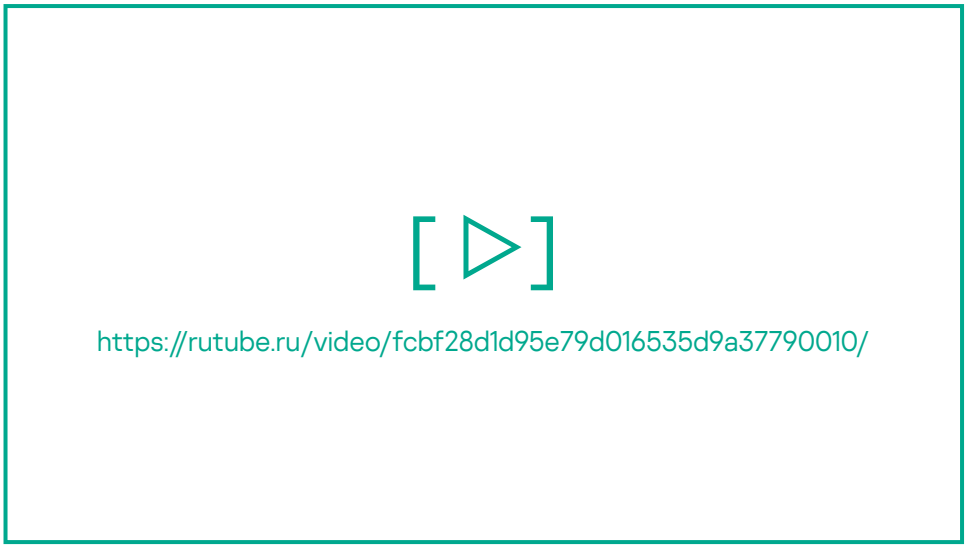
  2. В журнале коллектора не регистрируется ошибка.

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 LogAnalyzer. Доступные параметры парсинга событий описаны в таблице ниже.

При нормализации событий, помимо полей стандартной схемы событий LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer.

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 LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer 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.

LogAnalyzer 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.

- **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 LogAnalyzer, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна.

- **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.

Параметр	Описание
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 **ipfix**, **sql** и **normalizer**. Если парсинг события был выполнен успешно и тип полученных из сырого события данных совпадает с типом поля LogAnalyzer, 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 LogAnalyzer: • **Исходные данные** – названия полей исходного события, которые вы хотите преобразовать в поля события LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer. 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 LogAnalyzer.

Если размер поля события LogAnalyzer 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 LogAnalyzer, например, в качестве полей виджетов или для фильтрации и поиска событий. Список всех полей расширенной схемы событий, существующих в LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer 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 правилах обогащения. Вы не можете использовать это поле для детектирования источников 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 LogAnalyzer 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 LogAnalyzer.
   - 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 LogAnalyzer 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 LogAnalyzer поля расширенной схемы событий с информацией о них в файл, например, для передачи списка полей в другие инсталляции LogAnalyzer 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 LogAnalyzer из файла:

1. В веб-консоли LogAnalyzer 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 LogAnalyzer уже существует поле с таким названием и типом, такие поля из файла не будут импортированы.

Поля расширенной схемы событий будут импортированы из файла в LogAnalyzer. 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 LogAnalyzer 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 LogAnalyzer (нет зависимостей). Мы рекомендуем удалять поля расширенной схемы событий через некоторые время после того, как события, в которых использовалось поле, были гарантированно удалены из LogAnalyzer. После удаления поле не будет отображаться в подсказках событий.

Чтобы удалить поля расширенной схемы событий:

1. В веб-консоли LogAnalyzer 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 LogAnalyzer (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.

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 LogAnalyzer, 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.

- **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 LogAnalyzer, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если 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 LogAnalyzer. 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**.

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 LogAnalyzer, 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.

Параметр	Описание
Параметр	**Описание**
Параметр	**Описание**
Параметр	**Описание**
Целевое поле	Поле события LogAnalyzer, в которое требуется поместить данные. Обязательный параметр.

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 долно быть заполнено либо указано значение **Да** для параметра **Использовать сырое событие**.

- Блок фильтров – используется для формулирования сложных условий, которым должны удовлетворять события, поступающие в нормализатор.

  С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия (см. ниже).

  С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия.

  Условия и группы можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

Параметры условий фильтра:

- **Левый операнд** и **Правый операнд** – используются для указания значений, которые будет обрабатывать оператор.

  В левом операнде следует указывать исходное поле событий, поступающих в нормализатор. Например, если в окне **Основной парсинг событий** настроено сопоставление eventType - DeviceEventClass, то в окне **Дополнительный парсинг событий** на вкладке **Условия дополнительной нормализации** в поле левого операнда для фильтра следует указать eventType. Данные обрабатываются только как текстовые строки.

- Операторы:

  - **=** – полное совпадение левого и правого операндов.
  - **startsWith** – левый операнд начинается с символов, указанных в правом операнде.
  - **endsWith** – левый операнд заканчивается символами, указанными в правом операнде.
  - **match** – 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

LogAnalyzer 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.
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.
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway Syslog	regexp	Предназначен для обработки событий, поступающих от системы Barracuda Cloud Email Security Gateway по syslog.
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway Syslog	syslog	Предназначен для обработки части событий, поступающих от системы Barracuda Web Security Gateway версии 15.0 по syslog.
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
BeyondTrust's BeyondInsight	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по syslog.
Bloombase StoreSafe	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
BMC CorreLog	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Bricata ProAccel	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Brinqa Risk Analytics	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	Предназначен для обработки событий от системы Symantec Endpoint Protection.
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Brocade Fabric OS	[OOTB] Brocade Fabric OS Syslog	syslog	Предназначен для обработки событий Brocade Fabric OS версии 9.1, поступающих по syslog.
Canonical LXD	[OOTB] Canonical LXD Syslog	syslog	Предназначен для обработки событий, поступающих по syslog от системы Canonical LXD версии 5.18.
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 ASA	[OOTB] Cisco ASA and IOS Syslog	syslog	Предназначен для обработки событий, поступающих от сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), FWSM, NGIPS 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Cisco Firepower Threat Defense	[OOTB] Cisco ASA and IOS Syslog	syslog	Предназначен для обработки событий, поступающих от сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), FWSM, NGIPS по syslog.
Cisco Firewall Services Module (FWSM)	[OOTB] Cisco ASA and IOS Syslog	syslog	Предназначен для обработки событий, поступающих от сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), FWSM, NGIPS по syslog.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE Syslog	regexp	Предназначен для обработки событий системы Cisco Identity Services Engine (ISE), поступающих по syslog.
Cisco IOS	[OOTB] Cisco ASA and IOS Syslog	syslog	Предназначен для обработки событий, поступающих от сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), FWSM, NGIPS по syslog.
Cisco Next-Generation Intrusion Prevention System (NGIPS)	[OOTB] Cisco ASA and IOS Syslog	syslog	Предназначен для обработки событий, поступающих от сетевых устройств Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense (версия 7.2), FWSM, NGIPS 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 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 LogAnalyzer 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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) по syslog. Пакет доступен для LogAnalyzer версии 3.2 и выше.
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.
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 LogAnalyzer 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
F5 Advanced Web Application Firewall	[OOTB] F5 Advanced Web Application Firewall Syslog	regexp	Предназначен для обработки событий аудита, поступающих от системы F5 Advanced Web Application Firewall по syslog.
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
FFRI FFR yarai	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
FireEye CM Series	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
FireEye Malware Protection System	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Forcepoint NGFW	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Forcepoint SMC	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий, поступающих от системы Fortinet FortiAnalyzer версии 7.0, 7.2 по syslog в формате CEF.
Fortinet 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 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 FortiSOAR	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiWeb	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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 LogAnalyzer 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.
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 LogAnalyzer 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	syslog	Предназначен для обработки событий Indeed Privileged Access Manager версии 2.6.
Indeed SSO	[OOTB] Indeed SSO xml	xml	Предназначен для обработки событий системы Indeed SSO (Single Sign-On). Нормализатор поддерживает работу с LogAnalyzer 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 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 LogAnalyzer "dfi". Доступен в наборе ресурсов для LogAnalyzer версии 4.0 и выше.

Название системы	Название нормализатора	Тип	Описание нормализатора
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	syslog	Предназначен для обработки событий, поступающих от Kaspersky Endpoint Security for Linux (KESL) версии 12.2 в формате CEF по syslog.
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.
Kaspersky Industrial CyberSecurity for Networks 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 Syslog	syslog	Предназначен для обработки событий, поступающих от системы Kaspersky Industrial CyberSecurity for Networks версии 4.2 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 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 LogAnalyzer 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 в формате CEF по syslog.
Kaspersky Unified Monitoring and Analysis Platform (LogAnalyzer)	[OOTB] LogAnalyzer forwarding	json	Предназначен для обработки событий, перенаправленных из Kaspersky Unified Monitoring and Analysis Platform (LogAnalyzer).
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.
Kemptechnologies 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.
LogAnalyzer	[OOTB] LogAnalyzer forwarding	json	Предназначен для обработки событий, перенаправленных из LogAnalyzer.
LastLine Enterprise	[OOTB] LastLine Enterprise Syslog cef	syslog	Предназначен для обработки событий, поступающих от системы LastLine Enterprise версии 7.3, 8.1, 9.1 по syslog в формате CEF.
Libvirt	[OOTB] Libvirt Syslog	syslog	Предназначен для обработки событий Libvirt версии 8.0.0, поступающих по syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
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 LogAnalyzer 3.2	syslog	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, поступающих по syslog. Нормализатор поддерживает работу с событиями, обработанными коллектором LogAnalyzer версии 3.2 и выше.
Linux auditd	[OOTB] Linux auditd file for LogAnalyzer 3.2	regexp	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, хранящихся в файле. Нормализатор поддерживает работу с событиями, обработанными коллектором LogAnalyzer 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 LogAnalyzer версии 3.2 и выше.
Microsoft Active Directory Certificate Services (AD CS)	[OOTB] Microsoft Products for LogAnalyzer 3	xml	Предназначен для обработки событий журнала Active Directory Certificate Services (AD CS) в формате XML. Нормализатор [OOTB] Microsoft Products for LogAnalyzer 3 поддерживает работу с этим источником событий в LogAnalyzer 3.0.1 и выше.
Microsoft Active Directory Federation Service (AD FS)	[OOTB] Microsoft Products for LogAnalyzer 3	xml	Предназначен для обработки событий Microsoft AD FS. Нормализатор [OOTB] Microsoft Products for LogAnalyzer 3 поддерживает работу с данным источником событий в LogAnalyzer 3.0.1 и выше.
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products for LogAnalyzer 3	xml	Предназначен для обработки событий Microsoft AD DS. Нормализатор [OOTB] Microsoft Products for LogAnalyzer 3 поддерживает работу с данным источником событий в LogAnalyzer 3.0.1 и выше.
Microsoft Defender	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	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 LogAnalyzer версии 3.2 и выше.
Microsoft Exchange	[OOTB] Exchange CSV	csv	Предназначен для обработки журнала событий системы Microsoft Exchange. Источник событий – журналы MTA сервера Exchange.
Microsoft Hyper-V	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	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 IIS	[OOTB] IIS Log File Format	regexp	Обрабатывает события в формате, описанном по ссылке: https://learn.microsoft.com/en-us/windows/win32/http/iis-logging. Источник событий – журналы Microsoft IIS.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	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 LogAnalyzer 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 LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий модуля Microsoft Sysmon.
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки части событий из журналов Security, System, Application операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в LogAnalyzer от Kaspersky Endpoint Security для Windows 12.6 по syslog.
Microsoft → Windows → DNS-Server → Audit	[OOTB] Microsoft Products for LogAnalyzer 3	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	xml	Предназначен для обработки событий журнала Microsoft → Windows → Group Policy → Operational в формате XML.
Microsoft → Windows → PowerShell	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий журналов PowerShell операционной системы Microsoft Windows.
Microsoft → Windows → PowerShell-Operational	[OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки событий журналов PowerShell-Operational операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в LogAnalyzer от Kaspersky Endpoint Security для Windows 12.6 по syslog.
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 LogAnalyzer 2.1.3 и выше.
Microsoft SQL Server, Microsoft SQL Server Express	[OOTB] Microsoft Products for LogAnalyzer 3	xml	Предназначен для обработки событий MS SQL Server версии 2008 и новее.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products, [OOTB] Microsoft Products for LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	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 LogAnalyzer от Kaspersky Endpoint Security для Windows 12.6 по syslog.
Microsoft Windows Service Control Manager	[OOTB] Microsoft Products for LogAnalyzer 3 [OOTB] Microsoft Products via KES WIN	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 LogAnalyzer 3, [OOTB] Microsoft Products via KES WIN	xml	Предназначен для обработки части событий из журналов Security, System операционной системы Microsoft Windows Server. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в LogAnalyzer 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
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.

Название системы	Название нормализатора	Тип	Описание нормализатора
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 LogAnalyzer 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.
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 LogAnalyzer версии 3.2 и выше.
NIKSUN NetDetector	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
One Identity Privileged Session Management	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
OpenLDAP	[OOTB] OpenLDAP	regexp	Предназначен для построчной обработки части событий системы OpenLDAP версия 2.5, файл auditlog.ldif.
Open VPN	[OOTB] OpenVPN file	regexp	Предназначен для обработки журнала системы OpenVPN.
Oracle	[OOTB] Oracle Audit Trail	sql	Предназначен для обработки событий аудита БД, полученных коннектором непосредственно из базы данных Oracle.
OrionSoft Termit	[OOTB] OrionSoft Termit Syslog	syslog	Предназначен для обработки событий, поступающих от системы OrionSoft Termit версии 2.2 по syslog.
Orion soft zVirt	[OOTB] Orion Soft zVirt Syslog	regexp	Предназначен для обработки событий системы виртуализации Orion soft zVirt версии 3.1.
PagerDuty	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Networks NGFW	[OOTB] 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.
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 Sandbox	[OOTB] PTsecurity Sandbox	regexp	Предназначен для обработки событий системы PT Sandbox.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF	syslog	Предназначен для обработки событий, поступающих от системы PTsecurity (Web Application Firewall).

Название системы	Название нормализатора	Тип	Описание нормализатора
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 LogAnalyzer 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.
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.
SailPoint IdentityIQ	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
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 LogAnalyzer 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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Sendmail	[OOTB] Sendmail Syslog	syslog	Предназначен для обработки событий Sendmail версии 8.15.2, поступающих по syslog.
SentinelOne	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Skype for Business	[OOTB] Microsoft Products for LogAnalyzer 3	xml	Предназначен для обработки части событий из журнала системы Skype for Business, журнал Lync Server.
Snort	[OOTB] Snort 3 json file	json	Предназначен для обработки событий Snort версии 3 в формате JSON.
Sophos Central	[OOTB] Sophos Central Syslog	syslog	Предназначен для обработки части событий, поступающих от системы Sophos Central версии 1.2 по syslog в формате CEF от интеграционного скрипта Sophos-Central-SIEM-Integration.
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall	syslog	Предназначен для обработки событий, поступающих по syslog от межсетевого экрана Sonicwall TZ.
Solar webProxy	[OOTB] Solar WebProxy Syslog	regexp	Предназначен для обработки событий, поступающих от Solar webProxy версии 4.2 в формате siem-log по syslog.
SolarWinds DameWare MRC	[OOTB] SolarWinds DameWare MRC xml	xml	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 LogAnalyzer 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.
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.
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 LogAnalyzer 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_Intmov.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.

Название системы	Название нормализатора	Тип	Описание нормализатора
Trend Micro Deep Security	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Trend Micro NGFW	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Unbound	[OOTB] Unbound Syslog	syslog	Предназначен для обработки событий, поступающих по syslog от DNS-сервера Unbound.
UserGate	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF, поступающих от системы UserGate по syslog.
Varonis DatAdvantage	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
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 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	Предназначен для обработки событий межсетевых экранов WatchGuard Firebox, 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	Предназначенный для обработки части событий аудита системы Yandex Cloud. Нормализатор поддерживает обработку событий аудитного журнала уровня конфигурации: IAM (Yandex Identity and Access Management), Compute (Yandex Compute Cloud), Network (Yandex Virtual Private Cloud), Storage (Yandex Object Storage), Resourcemanager (Yandex Resource Manager).

Название системы	Название нормализатора	Тип	Описание нормализатора
Zabbix	[OOTB] Zabbix SQL	sql	Предназначен для обработки событий Zabbix версии 6.4.
Zecurion DLP	[OOTB] Zecurion DLP Syslog	regexp	Предназначен для обработки событий системы Zecurion DLP версии 12.0, поступающих по syslog.
ZEEK IDS	[OOTB] ZEEK IDS json file	json	Предназначен для обработки журналов системы ZEEK IDS в формате JSON. Нормализатор поддерживает события от ZEEK IDS версии 1.8.
Zettaset BDEncrypt	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	syslog	Предназначен для обработки событий в формате CEF.
АйТи Бастион – 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 LogAnalyzer 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.
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 LogAnalyzer 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	syslog	Предназначен для обработки событий от системы ViPNet Coordinator, поступающих по syslog.
Код безопасности - Континент	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	Предназначен для обработки журнала событий устройств Континент IPS/IDS.
Код безопасности - Континент	[OOTB] Continent SQL	sql	Предназначен для получения событий системы Континент из базы данных.
Код Безопасности SecretNet 7	[OOTB] SecretNet SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы SecretNet.

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 системы Единый центр управления (ЕЦУ) Dallas Lock (версии 4.0) 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	Предназначен для обработки событий системы СКДПУ НТ Шлюз доступа версии 7.0, 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 LogAnalyzer 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 LogAnalyzer и с полями расширенной схемы событий. Таким образом вы можете уменьшить количество схожих событий, передаваемых в хранилище, 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.

Доступные параметры правила агрегации

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.

Параметр	Описание
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.
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

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	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.

Параметр	Описание
	• **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. • **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 .

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 LogAnalyzer:

- 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.

- 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 Основные параметры

Параметр	Описание

Тип источника данных

Обязательный параметр.

Раскрывающийся список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры:

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. 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 LogAnalyzer, 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** (доступно только в коммерческой версии LogAnalyzer)

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** (доступно только в коммерческой версии LogAnalyzer)

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. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события LogAnalyzer, 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 LogAnalyzer. 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 LogAnalyzer, 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** (доступно только в коммерческой версии LogAnalyzer)
```

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 LogAnalyzer.
- **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 LogAnalyzer 3.4.1. С помощью переключателя можно включить отправку коллектором LogAnalyzer рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

- **cybertrace** (доступно только в коммерческой версии LogAnalyzer)

  Для систем с большой нагрузкой на коллектор 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]**), LogAnalyzer 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 LogAnalyzer. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро LogAnalyzer.
  - **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 LogAnalyzer с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий LogAnalyzer, 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** (доступно только в коммерческой версии LogAnalyzer)

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 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), 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главный администратор также должен принять дополнительное лицензионное соглашение KSN в разделе **Kaspersky Security Network** (**Параметры** → **Интеграции** → **AI-сервисы** → **Kaspersky Security Network**).

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 берётся 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 LogAnalyzer 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, LogAnalyzer 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, LogAnalyzer 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 умочанию: `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 со списком параметров, которые нужно отправить в запросе в KSN для получения заключения, и списком соответствующих полей событий LogAnalyzer. 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, LogAnalyzer 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, LogAnalyzer 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.

  - **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize.

  Для каждого обязательного параметра укажите в таблице соответствующее ему поле события LogAnalyzer.

Параметр	Описание
Параметр	Описание
Параметр	Описание
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.
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**

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.
- **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 .

Предустановленные правила обогащения

В поставку LogAnalyzer включены перечисленные в таблице ниже правила обогащения.

Предустановленные правила обогащения

Название правила обогащения	Описание
[OOTB] KATA alert	Используется для обогащения событий, поступивших от KATA в виде гиперссылки на алерт. Гиперссылка размещается в поле DeviceExternalId.

Фильтры

Фильтры позволяют отбирать события на основании указанных условий. В сервисе коллектора фильтры используются для отображения событий, которые вы хотите передавать в LogAnalyzer. События, удовлетворяющие условия фильтра, будут переданы в LogAnalyzer для дальнейшей обработки.

Вы можете использовать фильтры в следующих сервисах и функциях LogAnalyzer:

- Коллектор.
- Хранилище.

- Правила обогащения.
- Правила агрегации.
- Точки назначения.

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.

Параметр	Описание
	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.

Параметр	Описание
	• **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.
<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.

Параметр	Описание
	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.

Параметр	Описание
	• **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. • **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 "словарь"	Тип "таблица"	Тип "TI"	Тип "константа"	Тип "список"
=	L, R	L, R	L, R	L, R	R	R
>	L, R	L, R	L, R	L	R	—
>=	L, R	L, R	L, R	L	R	—
<	L, R	L, R	L, R	L	R	—
<=	L, R	L, R	L, R	L	R	—
inSubnet	L, R	L, R	L, R	L, R	R	R
contains	L, R	L, R	L, R	L, R	R	R
startsWith	L, R	L, R	L, R	L, R	R	R
endsWith	L, R	L, R	L, R	L, R	R	R
match	L	L	L	L	R	R
hasVulnerability	L	L	L	—	—	—
hasBit	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—
inCategory	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—
inActiveDirectoryGroup	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
`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 LogAnalyzer.

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 LogAnalyzer 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 учётной записи в ОС Windows.
[OOTB][AD] Account Deleted	Выбирает события удаления учётной 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.

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

Эта функциональность доступна только в коммерческой версии LogAnalyzer.

Описание параметров

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами LogAnalyzer. Словари могут использоваться в следующих сервисах и функциях LogAnalyzer:

- Коллектор.
- 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 LogAnalyzer. 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 LogAnalyzer. Для просмотра содержимого таких словарей содержимое необходимо экспортировать в формат CSV. Если CSV-файл отредактировать и снова импортировать в LogAnalyzer, 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 LogAnalyzer 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.

Коннекторы

Коннекторы используются для установления соединений между сервисами LogAnalyzer, 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 LogAnalyzer 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.
- 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 Систем Управления Базами Данных (СУБД). LogAnalyzer поддерживает работу с несколькими **типами баз данных**. При создании коннектора с типом **sql** вам нужно указать значения для общих параметров коннектора и отдельных параметров подключения к базе данных.

  Программа поддерживает работу со следующими типами баз данных SQL:

  - SQLite.
  - MariaDB 10.5 и выше.
  - MsSQL.
  - MySQL 5.7 и выше.
  - PostgreSQL.
  - Cockroach.
  - Oracle.
  - Firebird.

- 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 LogAnalyzer 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 – используется для получения данных Kaspersky Digital Footprint Intelligence по API.

Некоторые типы коннекторов (например, tcp, sql, wmi, wec и etw) поддерживают шифрование с использованием протокола TLS. LogAnalyzer поддерживает протокол TLS версии 1.2 или 1.3. При включении режима TLS для этих коннекторов подключение осуществляется по следующему алгоритму:

- Если LogAnalyzer используется в качестве клиента:

  1. LogAnalyzer 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, LogAnalyzer установит соединение с сервером.
     - Если сервер отвечает на запрос, используя TLS 1.1, LogAnalyzer закроет соединение с сервером.

- Если LogAnalyzer используется в качестве сервера:

  1. Клиент отправляет запрос на соединение с LogAnalyzer 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, LogAnalyzer закроет соединение.
     - Если в запросе клиента используется протокол TLS 1.2 или 1.3, LogAnalyzer ответит на запрос выбранной версией протокола TLS и криптонабора.

Просмотр параметров коннектора

Чтобы просмотреть параметры коннектора:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer типов коннекторов.

Коннектор, тип internal

Коннекторы с типом **internal** используются для приема данных от сервисов LogAnalyzer 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, 1c-xml или 1c-log, на шаге Парсинг событий в таблице **Сопоставление** вы можете передать в поле события LogAnalyzer название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:
  - `$kuma_fileSourceName` – передать в поле события LogAnalyzer название обрабатываемого коллектором файла.
  - `$kuma_fileSourcePath` – передать в поле события LogAnalyzer путь к обрабатываемому коллектором файлу.

  Когда вы используете коннектор с типом **file**, **1c-xml** или **1c-log**, 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`. Вы можете добавить несколько значений и удалить значения. Для добавления значения нажмите на кнопку **+ Добавить**. Для удаления значения 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.

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.

Параметр	Описание
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.
	LogAnalyzer классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие
	`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:`.

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 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.
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 LogAnalyzer 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 LogAnalyzer. Вы можете просмотреть в метриках LogAnalyzer, сколько оперативной памяти сервера использует коллектор LogAnalyzer. 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 LogAnalyzer.
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 LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer. • **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 LogAnalyzer 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 LogAnalyzer 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.

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 с **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. LogAnalyzer классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие `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:`.
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**.

Параметр	Описание
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор LogAnalyzer 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 LogAnalyzer. Вы можете просмотреть в метриках LogAnalyzer, сколько оперативной памяти сервера использует коллектор LogAnalyzer. 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 LogAnalyzer.
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 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.

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. LogAnalyzer 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**.
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.

Параметр	Описание
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.
	• **С верификацией** – использовать шифрование TLS с верификацией сертификата, подписанного корневым сертификатом LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer.
	• **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 LogAnalyzer (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 LogAnalyzer>" -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 LogAnalyzer в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов LogAnalyzer 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 LogAnalyzer 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?

Параметр	Описание
	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.

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. LogAnalyzer 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 LogAnalyzer 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.
Топик	Тема сообщений Kafka. Максимальная длина темы составляет до 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: до 255 символов. Вы можете использовать символы a–z, A–Z, 0–9, ".", "_", "-".

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.
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**.

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 LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer.
	• **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 LogAnalyzer (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 LogAnalyzer>" -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 LogAnalyzer в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов LogAnalyzer 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.

Параметр	Описание
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, сек. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания чтения	Время ожидания операции чтения, сек. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания записи	Время ожидания операции записи, сек. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Интервал обновления состояния группы	Интервал обновления состояния группы, сек. Не может превышать время сессии. Рекомендуемое значение: 1/3 от времени сессии. Максимально допустимое значение: 2147483647. По умолчанию 3 секунды.
Время сессии	Время сессии, сек. Максимально допустимое значение: 2147483647. По умолчанию 10 секунд.
Максимальное время обработки одного сообщения	Максимальное время обработки одного сообщения одним потоком, миллисекунды. Максимально допустимое значение: 2147483647. По умолчанию 100 миллисекунд.
Включить автокоммит	По умолчанию включено.
Интервал автокоммита	Интервал автокоммита, сек. По умолчанию 1 секунда. Максимально допустимое значение: 18446744073709551615. Допустимо указать любое положительное число.
PFX секрет	Секрет с типом pfx. Поле доступно для заполнения, если для параметра **Авторизация** выбрано значение **PFX**. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Обязательное поле.
Секрет	Секрет с типом credentials. Поле доступно для заполнения, если для параметра **Авторизация** выбрано значение **Обычная**. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Обязательное поле.

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.

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.

Параметр	Описание
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.
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**.

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 LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer. • **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 LogAnalyzer 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 LogAnalyzer 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 Систем Управления Базами Данных (СУБД). LogAnalyzer поддерживает работу с несколькими **типами баз данных**. 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.

Программа поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MariaDB 10.5 и выше.
- MsSQL.
- MySQL 5.7 и выше.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.

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 подключения к базе данных:

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><th>Параметр</th><th>Описание</th></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>%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**. LogAnalyzer 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 LogAnalyzer.

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: `?`.

  LogAnalyzer 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 LogAnalyzer, 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 **Столбец идентификатора** 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 **Столбец идентификатора**.

- **Обычная**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Столбец идентификатора** указан ID секрета типа credentials.

- **PublicPKI**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Столбец идентификатора** 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 LogAnalyzer 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 LogAnalyzer название обрабатываемого коллектором файла.

- `$kuma_fileSourcePath` – передать в поле события LogAnalyzer 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 пусты • `'?'` – соответствует любому одиночному символу. Диапазоны символов: • `[0-9]` – числа; • `[a-zA-Z]` – буквы латинского алфавита. Параметр | Описани 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

Параметр	Описание
	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/

Параметр	Описание

	Приведенные префиксы используются системой в качестве регулярных выражений для прове 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/`
	
	Ограничение количества отслеживаемых файлов по маске
	
	Количество одновременно отслеживаемых файлов по маске может быть ограничено парамет Ядра `max_user_watches`. Для просмотра значения параметра выполните команду:
	
	`cat /proc/sys/fs/inotify/max_user_watches`
	
	Если количество файлов для отслеживания превышает значение параметра `max_user_watch` коллектор больше не сможет считывать события из 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 превышало значение параметра `max_user_watches`, ил 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 LogAnalyzer выполнила с ним действие, указанное в раскрывающемся списке **Действие после таймаута**. Значение по умолчанию: `0` – если файл не обновляется, LogAnalyzer не вы ним никакого действия. Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Дополнительные параметры** в поле **Интер запросов, мс**.
Действие после таймаута	Действие, которое LogAnalyzer выполняет с файлом по прошествии времени, указанного в поле **Время ожидания изменений,** • **Ничего не делать**. Значение по умолчанию. • **Добавление суффикса** – добавить к названию файла расширение .kuma_processed и не обрабатывать файл даже при его • **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 меж 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. LogAnalyzer классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены следующие з `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:`.
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 LogAnalyzer 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 LogAnalyzer. Вы можете просмотреть в метриках LogAnalyzer, сколько оперативной памяти сервера использует коллектор LogAnalyzer. 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 LogAnalyzer.
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.

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

Параметр	Описание
	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/

Параметр	Описание
	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

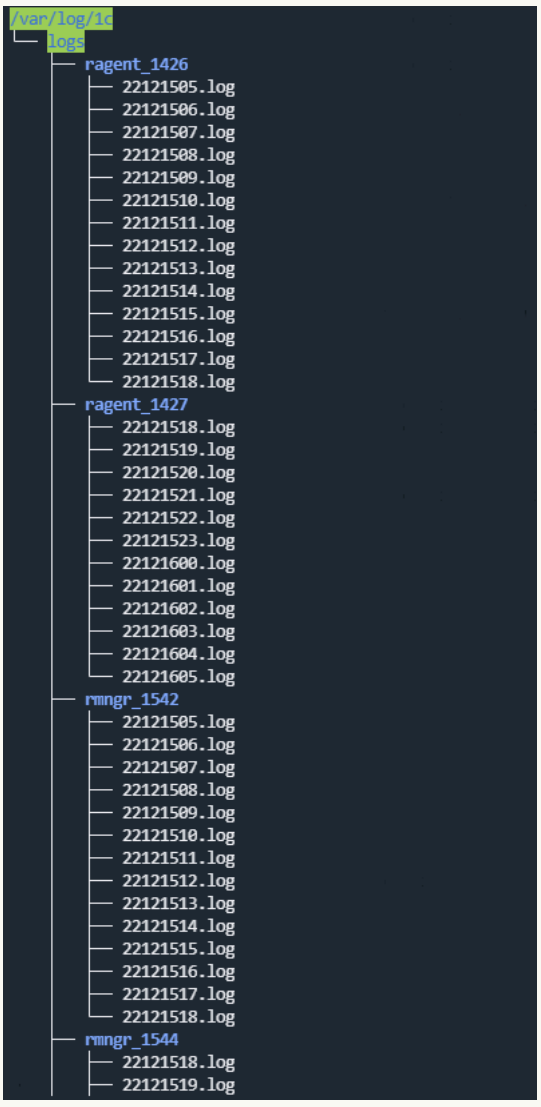
Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер 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

     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

Параметр	Описание
	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/

Параметр	Описание
	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 и отбрасываются все файлы, измененные раньше, чем последний прочитанный.

   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

- 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 LogAnalyzer, 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

Параметр	Описание
	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/

Параметр	Описание
	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.
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

<table>
<tr><th>Параметр</th><th>Описание</th></tr>
<tr><td>Название</td><td>Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode.
Обязательный параметр.</td></tr>
<tr><td>Тенант</td><td>Название тенанта, которому принадлежит ресурс.
Обязательный параметр.</td></tr>
<tr><td>Тип</td><td>Тип коннектора – ftp.
Обязательный параметр.</td></tr>
<tr><td>Теги</td><td>Теги для поиска ресурса.
Необязательный параметр.</td></tr>
<tr><td>URL</td><td>URL-адрес файла или маски файлов, начинающийся со схемы <code>'ftp://'</code>. Для маски файлов вы можете использовать символы <code>* ? [...]</code>.
Шаблоны масок для файлов

Маски:
• <code>'*'</code> – соответствует любой последовательности символов;
• <code>'[' ['^'] { <диапазон символов> } ']'</code> – класс символов (не должен быть пустым);
• <code>'?'</code> – соответствует любому одиночному символу.

Диапазоны символов:
• <code>[0-9]</code> – числа;
• <code>[a-zA-Z]</code> – буквы латинского алфавита.

<table><tr><th>Параметр</th><th>Описание</th></tr><tr><td>Пример:
Маски можно использовать как в путях Linux, так и Windows с заменой прямой косой черты на обратную:
• Для Linux:
◦ <code>/var/log/*som?[1-9].log</code>
◦ <code>/mnt/dns_logs/*/dns.log</code>
◦ <code>/mnt/proxy/access*.log</code>
• Для Windows:
◦ <code>C:\var\log\test123.log</code>
◦ <code>D:\data*\report?.txt</code></td><td></td></tr></table>
Если URL-адрес не содержит номер порта FTP-сервера, автоматически указывается номер порта <code>21</code>.
Обязательный параметр.</td></tr>
<tr><td>Секрет</td><td></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**.

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.
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.

Параметр	Описание
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.
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`. Обязательный параметр. • **Домен** – название домена, в котором расположено удаленное устройство, например, `example.com`. 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 LogAnalyzer 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. LogAnalyzer 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**.
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 LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer.
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 LogAnalyzer:

- Для запуска агента LogAnalyzer на удаленном устройстве вам нужно использовать учетную запись с правами Log on as a service.
- Для получения событий от агента LogAnalyzer 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.
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 LogAnalyzer 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**.

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 LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer.
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.

Параметр	Описание
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. • **С верификацией** – использовать шифрование TLS с верификацией сертификата, подписанного корневым сертификатом LogAnalyzer. Корневой сертификат и ключ LogAnalyzer создаются автоматически при установке программы и помещаются на сервер Ядра LogAnalyzer в директорию /opt/kaspersky/kuma/core/certificates. Устаревший режим шифрования, не рекомендуется к использованию. Будет исключен в будущих версиях LogAnalyzer.
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`. LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer 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.

Параметр	Описание
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 ✕.
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`. LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer, 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 LogAnalyzer.
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 LogAnalyzer 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. LogAnalyzer 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
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.
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 LogAnalyzer (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 LogAnalyzer>" -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 LogAnalyzer в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	
	Для использования сертификатов LogAnalyzer 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.
Тип	Тип коннектора – **elastic**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
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 LogAnalyzer 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 LogAnalyzer. 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**.

Параметр	Описание
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.
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.

Параметр	Описание

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`.
	LogAnalyzer не позволяет сохранить ресурс или сервис, если в поле URL есть знак табуляции или пробел.
	Обязательный параметр.

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**.

Предустановленные коннекторы

В поставку LogAnalyzer включены перечисленные в таблице ниже 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 Traffic Monitor SQL	Собирает события из СУБД системы InfoWatch Traffic Monitor. 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] SecretNet SQL	Собирает события из СУБД системы SecretNet SQL. Для использования необходимо настроить параметры соответствующего типа секрета.

Секреты

Секреты используются для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые должны использоваться LogAnalyzer для взаимодействия с внешними службами. Если секрет хранит данные учётной записи, такие как логин и пароль, то при подключении коллектора к источнику событий учётная запись, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

Секреты можно использовать в следующих сервисах и функциях LogAnalyzer:

- 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, учётная 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** (доступно только в коммерческой версии LogAnalyzer) – 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. LogAnalyzer 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 LogAnalyzer.

    Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.

  - Закрытый ключ шифрования соединения – RSA-ключ сервера LogAnalyzer.

    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 LogAnalyzer к ClickHouse. При выборе этого варианта требуется указать секрет, содержащий закрытый ключ PEM, закодированный в base64, и открытый ключ.

Предустановленные секреты

В поставку LogAnalyzer включены перечисленные в таблице ниже секреты.

Предустановленные секреты

Название секрета	Описание
[OOTB] Continent SQL connection	Хранит конфиденциальные данные и параметры подключения к БД АПКШ Континент. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MSSQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MySQL Connection	Хранит конфиденциальные данные и параметры подключения к БД MySQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.

[OOTB] Oracle Audit Trail SQL Connection	Хранит конфиденциальные данные и параметры подключения к БД Oracle. Для использования необходимо указать логин и пароль БД.
[OOTB] SecretNet SQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL системы SecretNet. Для использования необходимо указать логин и пароль БД.

Аналитика

LogAnalyzer предоставляет обширную аналитику по данным, доступным программе из следующих источников:

- События в хранилище
- Активы
- Сведения из коллекторов о количестве обработанных событий
- Метрики

Вы можете настроить и получать аналитику в разделах **Панель мониторинга**, **Отчеты**, **Состояние источников** веб-интерфейса LogAnalyzer. Для построения аналитики используются только данные из тенантов, к которым у пользователя есть доступ.

Формат даты зависит от языка локализации, выбранного в настройках программы. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Работа с событиями

В разделе **События** веб-интерфейса LogAnalyzer вы можете просматривать полученные программой события. В таблице событий отображаются данные, полученные после выполнения SQL-запроса.

Формат даты события зависит от языка локализации, выбранного в настройках программы. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Фильтрация и поиск событий

По умолчанию в разделе **События** веб-интерфейса LogAnalyzer 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 LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer возвращает соответствующие им названия.

Подробнее об SQL см. в справке ClickHouse. Также об SQL-операторах и функциях, поддерживаемых в LogAnalyzer, см. использование операторов в LogAnalyzer и поддерживаемые функции.

Выбор хранилища

События, которые отображаются в веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer Default.
- Пространство LogAnalyzer Audit, если выбран тенант Main и если в этом пространстве есть хотя бы одно событие аудита.

LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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.

   - **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.
   - **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**.

   В таблице отобразятся результаты поиска по сформированному SQL-запросу.

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 LogAnalyzer 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 LogAnalyzer.

   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**.

   Отобразится таблица событий, соответствующих условиям вашего запроса. При необходимости вы можете отфильтровать события 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.
`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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer вы можете настроить отображение событий, относящихся к определенному временному периоду.

Чтобы отфильтровать события по периоду:

1. В разделе **События** веб-интерфейса LogAnalyzer 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 слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

     Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

   - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

     В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени 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 LogAnalyzer 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**.

Группировка событий

После получения списка событий часто возникает потребность разделить полученные события по группам, чтобы локализовать событие информационной безопасности. В LogAnalyzer 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 кнопку **-**.
- 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, рестроспективная проверка 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, LogAnalyzer 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.

Сохранение и выбор конфигураций фильтра событий

В LogAnalyzer 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 LogAnalyzer и доступны всем пользователям LogAnalyzer выбранного тенанта.

Чтобы сохранить текущие настройки фильтра, запроса и периода:

1. В разделе **События** веб-интерфейса LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

Поддерживаемые функции ClickHouse

В LogAnalyzer 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 программы 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 приложении.
- По ссылке с именем коллектора в поле **Service** просмотреть параметры сервиса, зарегистрировавшего событие.

- 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer они не отображались из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. В разделе **События** веб-интерфейса LogAnalyzer 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 LogAnalyzer можно настроить отображаемый набор полей событий и порядок их отображения. Выбранную конфигурацию можно сохранить.

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, 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 LogAnalyzer 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.

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.

Формирование SQL-запроса с помощью SQL-функций LogAnalyzer

SQL-функции LogAnalyzer 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.

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)`

`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.

Функция	Поле события	Поле актива	Описание

`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.

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, ук
				запросе.
				Для значений, которые являю
				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 являю
				надо указывать строку с нео
				числом.
				Например:
				`lookup_assets(DeviceAss`
				`'>', '50')`
				Значения, которые являются
				указывать в следующих фор
				• Количество секунд:
				`lookup_assets(Device`
				`lastVisible, '>', '1`
				• Количество миллисекун
				`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`

Тип функции	Поле события	Поле актива	Оператор	Описание

		`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'`

		`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 являю надо указывать строку с нео числом. Например: lookup_accounts(SourceA employee_id, '=', '1545

Тип функции	Поле события	Поле актива	Оператор	Описание
		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
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 и 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 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 отображении данных на панели мониторинга или в отчетах. С помощью набора ресурсов LogAnalyzer можно выполнить категоризацию некоторых типов событий для определенных типов источников событий.

Для категоризации событий используются следующие типы ресурсов LogAnalyzer:

- 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 LogAnalyzer.
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 LogAnalyzer 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 Jflow и другое.
OS	События, поступающие от операционной системы, например, Windows, Linux, Cisco IOS, HP-UX и другое. Провайдером событий могут быть как штатные инструментыоперационной 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer формируется событие аудита.

Теперь необходимо выдать пользователям права доступа к созданному набору пространств.

Изменение набора пространств

Чтобы изменить набор пространств:

1. В веб-консоли LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer установлен набор по умолчанию, явно указывающий только конечное число пространств. Также в LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

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 LogAnalyzer. 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.

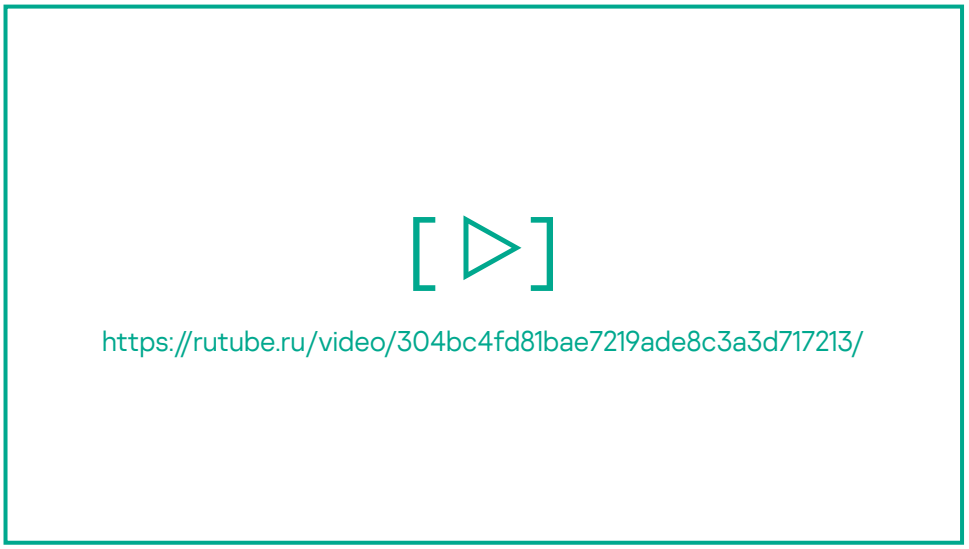
Создавать, изменять параметры и удалять панели мониторинга могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня и Аналитик первого уровня. Пользователи с учетными записями всех ролей могут просматривать панели мониторинга и назначать панели мониторинга 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 LogAnalyzer 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.
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 LogAnalyzer 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 слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

     Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

   - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

     В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени 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 LogAnalyzer хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме **now**), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 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. Нажмите **Применить**.

11. 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 ⠿, расположенного рядом с левым верхним углом виджета. Если вам необходимо изменить размер виджета, вы можете сделать это с помощью значка ⤡, 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 ⋮ 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.

12. Нажмите **Создать**.

Панель мониторинга создана и отображается в разделе **Панели мониторинга** веб-интерфейса LogAnalyzer.

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**.

   LogAnalyzer 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 LogAnalyzer.

Выбор панели мониторинга в качестве панели мониторинга по умолчанию

Чтобы выбрать панель мониторинга, которая будет отображаться по умолчанию:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer, чтобы в раскрывающемся списке просмотреть перечень доступных панелей мониторинга.

Удаление панели мониторинга

Чтобы удалить панель мониторинга:

1. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer.

Если в выбранные для слайд-шоу панели мониторинга вносятся изменения, эти изменения будут автоматически отображаться в запущенных сессиях слайд-шоу.

Предустановленные панели мониторинга

LogAnalyzer поставляется с набором предустановленных панелей мониторинга. По умолчанию для предустановленных панелей мониторинга указан период обновления **Никогда**. Вы можете изменить эти панели мониторинга при необходимости.

Предустановленные панели мониторинга

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.

Название панели мониторинга	Описание виджетов в составе панелей мониторинга
[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.
[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.

Название панели мониторинга	Описание виджетов в составе панелей мониторинга
[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 LogAnalyzer 3.4.1. Виджеты будут корректно отображать информацию при использовании нормализатора [OOTB] KSMG 2.1+ syslog CEF.

Универсальность панелей мониторинга

Панель мониторинга в LogAnalyzer 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 LogAnalyzer, 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 LogAnalyzer.

   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 LogAnalyzer.
- 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 LogAnalyzer.

   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 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 LogAnalyzer.

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 LogAnalyzer.

При развертывании LogAnalyzer в отказоустойчивом варианте временная зона сервера Ядра LogAnalyzer 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. Откройте веб-интерфейс LogAnalyzer и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.

   - **Ресурсы** → **Список**. Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В зависимости от выбранного раздела выполните одно из следующих действий:

   - В разделе **Отчеты** → **Шаблоны** нажмите на кнопку **Создать**, расположенную над таблицей со списком шаблонов отчетов.

   - В разделе **Ресурсы** → **Список** нажмите на кнопку **Создать** и выберите **Шаблон отчетов** в списке ресурсов.

3. В открывшемся окне укажите уникальное название шаблона отчета. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В раскрывающемся списке **Тенант шаблона** выберите тенант, которому будет принадлежать создаваемый шаблон отчета.

5. В раскрывающемся списке **Собирать данные от тенантов** выберите один или несколько тенантов. На основании данных выбранных тенантов далее будут сформированы отчеты.

6. При необходимости в раскрывающемся списке **Временной интервал** выберите период, по которому требуется аналитика, одним из следующих способов:

   - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

     Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

   - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

     В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени 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 LogAnalyzer хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме **now**), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 в UTC вчерашнего дня, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

7. При необходимости в поле **Срок хранения** укажите, в течение какого времени следует хранить сформированные по этому шаблону отчеты.

   По умолчанию указано значение: 3 месяца.

8. При необходимости в раскрывающемся списке **Теги** выберите нужные теги для шаблона отчета.

9. При необходимости добавьте описание шаблона отчета.

10. Нажмите **Сохранить**.

11. В открывшемся окне при необходимости можно поменять логотип шаблона отчетов, нажав на ссылку **Загрузите файл**. В окне загрузки укажите файл изображения для логотипа. Изображение должно быть в формате JPG, PNG или GIF и размером не более 3 МБ.

    Добавленный логотип будет отображаться в отчете вместо логотипа LogAnalyzer.

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 по окну с помощью значка перетаскивания ⠿, расположенного рядом с левым верхним углом виджета. Если вам необходимо изменить размер виджета, вы можете сделать это с помощью значка растяжения ⤡, который появляется при наведении указателя мыши на правый нижний угол виджета.

    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**.

    Новый шаблон отчета создан и отображается на вкладках **Отчеты** → **Шаблоны** и **Ресурсы** → **Список** веб-интерфейса LogAnalyzer. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, нужно настроить расписание.

Настройка расписания отчетов

Чтобы настроить расписание отчетов:

1. Откройте веб-интерфейс LogAnalyzer 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 LogAnalyzer 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.
   - 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 LogAnalyzer.

Копирование шаблона отчета

Чтобы создать копию шаблона отчета:

1. Откройте веб-интерфейс LogAnalyzer 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 LogAnalyzer.

Удаление шаблона отчета

Чтобы удалить шаблон отчета:

1. Откройте веб-интерфейс LogAnalyzer 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 LogAnalyzer и перейдите в один из следующих разделов:

   - **Отчеты** → **Шаблоны**.
   - **Ресурсы** → **Список**. Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в LogAnalyzer.

2. С помощью флажка выберите шаблон отчета для экспорта.

3. Нажмите на кнопку **Экспортировать**, расположенную над таблицей со списком шаблонов отчетов.

4. В открывшейся боковой панели выполните следующие действия:

   a. Укажите пароль к файлу с экспортируемыми ресурсами. Пароль должен 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.

5. Нажмите на кнопку **Экспортировать**.

При экспорте шаблонов отчета необходимо учитывать следующее:

- Шаблоны отчетов экспортируются без информации о тенантах, хранилищах и пространствах, поскольку эти параметры устанавливаются отдельно для каждого развертывания LogAnalyzer.
- Виджеты шаблона отчета также экспортируются без информации о тенантах, хранилищах и пространствах.

Чтобы импортировать шаблон отчета:

1. Откройте веб-интерфейс LogAnalyzer и перейдите в один из следующих разделов:

   - **Отчеты → Шаблоны**.
   - **Ресурсы → Список**. Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в LogAnalyzer.

2. С помощью флажка выберите шаблон отчета для импорта.

3. Нажмите на кнопку **Импортировать**, расположенную над таблицей со списком ресурсов.

4. В открывшейся боковой панели в раскрывающемся списке **Тенант** выберите тенант, в который вы хотите импортировать шаблон отчета.

5. Выберите источник импорта: **Файл** или **Репозиторий**.

6. В зависимости от выбранного источника импорта, выполните следующие шаги:

   a. Если вы выбрали **Файл** в качестве источника импорта, выполните следующие действия:

      - Укажите пароль к импортируемому файлу.
      - С помощью кнопки **Выбрать файл** выберите файл для импорта.
      - С помощью флажков выберите ресурсы, которые вы хотите импортировать.

   b. Если вы выбрали **Репозиторий** в качестве источника импорта, в открывшейся таблице выберите один или несколько пакетов репозитория.

7. Нажмите на кнопку **Импортировать**.

8. При необходимости устраните конфликты между импортированными из файла и существующими ресурсами.

При импорте шаблона отчета необходимо учитывать следующее:

- Если шаблон импортируется в любой тенант, то тенант импортируемого шаблона отчета указывается в качестве тенанта ресурса и тенанта источника данных.
- После импорта ресурсов необходимо указать пространства для виджетов с событиями и при необходимости расширить список тенантов.

Универсальность шаблона отчетов

Шаблон отчета в LogAnalyzer 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, LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчетов нажмите на название сформированного отчета.

   Откроется окно с виджетами, отображающими аналитику отчетов. При нажатии на заголовок виджета открывается соответствующий раздел веб-интерфейса LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. С помощью флажка выберите сформированный отчет в таблице со списком сформированных отчетов.
3. В раскрывающемся списке **Сохранить как**, расположенном над таблицей, выберите нужный формат: HTML, PDF, CSV, разделенный CSV, Excel.

   Отчет сохраняется в папку загрузки, настроенную в вашем браузере.

Отчет также можно сохранить в выбранном формате при просмотре.

Обновление отчетов

Чтобы обновить сформированный отчет:

1. Откройте веб-интерфейс LogAnalyzer 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 LogAnalyzer 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 приложения. В LogAnalyzer доступны виджеты типа **События**, **то есть** виджеты для создания аналитики на основе событий.

В таблице событий, в области деталей событий, 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 LogAnalyzer 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 вы можете перейти в соответствующий раздел веб-интерфейса LogAnalyzer.

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 LogAnalyzer 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.

Под значком периода отображается количество событий, сгруппированных по выбранным критериям за период отображения данных на виджетах.

Пример:
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.

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 LogAnalyzer 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.

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 LogAnalyzer 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 пользователи, хосты. Градиентная заливка к такому графику не применяется.

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 LogAnalyzer 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 LogAnalyzer 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 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:
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 LogAnalyzer 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 LogAnalyzer 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 LogAnalyzer 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 **ОК**.
7. Нажмите на кнопку **Сохранить**.

Виджет будет удален.

Виджет События

Вы можете использовать виджет **События** для получения необходимой аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, расположенные на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Тип графика. Доступны следующие типы графиков: • **Круговая диаграмма**. • **Столбчатая диаграмма**. • **Счетчик**. • **Линейная диаграмма**. • **Таблица**. • **Календарная диаграмма**. • **Сложенная столбчатая диаграмма**. • **Спидометр**.
Формат	Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. Параметр доступен для графика типа **Сложенная столбчатая диаграмма**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Вид временной диаграммы	Формат отображения временных данных: **Столбчатая диаграмма** или **Линейная диаграмма**. Параметр доступен для графика типа **Календарная диаграмма**. При выборе формата **Столбчатая диаграмма** данные по умолчанию отображаются в виде вертикальных столбцов. Если SQL-запрос содержит дополнительное поле с псевдонимом `category`, столбчатая диаграмма будет представлена в виде сложенной диаграммы, то есть с разбивкой каждого столбца по значениям этого поля. При выборе формата **Линейная диаграмма** данные отображаются в виде одной или нескольких (в зависимости от запроса) ломаных линий, соединяющих точки на временной оси. По умолчанию выбран формат **Столбчатая диаграмма**.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Показывать данные за предыдущий период	Включение отображения данных сразу за два периода: за текущий и за предыдущий. При использовании графика типа **Сложенная столбчатая диаграмма** параметр **Показывать данные за предыдущий период** будет учитываться, если в запросе указаны стандартные псевдонимы `value`, `category`, `metric`. Если же в запросе вместо стандартной метрики `metric` используется пользовательский расчет метрик с нестандартными псевдонимами, то параметр **Показывать данные за предыдущий период** учитываться не будет.

Параметр	Описание
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.

Параметр	Описание
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.
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

Параметр	Описание
	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:/yndex.ru] 10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru] Главный администратор LogAnalyzer добавил поле расширенной схемы событий в разделе LogAnalyzer **Параметры → Другое → Поля расширенной схемы событий**. В нормализаторе LogAnalyzer настроено сопоставление полей **ReqUrls** и **SA.urls**. В LogAnalyzer 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 LogAnalyzer 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.

Параметр	Описание

	Пример с использованием переменных
	
	Пример SQL-запроса с использованием локальной переменной:
	
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	
	В этом запросе использована локальная переменная `$Name`. В эту переменную будет подставляться значение из поля события Name. Вы сможете применить переменную, нажав на значок воронки ( ) на виджете. В открывшемся окне вы сможете выбрать значение для переменной. Виджет отфильтрует выборку по выбранному значению поля Name.
	
	Обратите внимание, если в SQL-запросе вы прописываете переменную для поля, которое принимает числовое значение, такое значение надо преобразовать в строку. Для этого используйте функцию `toString`. В противном случае SQL-запрос вернет ошибку. Пример:
	
	`SELECT count(ID) AS \`metric\`, SourcePort AS \`value\` FROM \`events\` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	
	В этом запросе поле события SourcePort имеет числовое значение, поэтому оно преобразовано в строку: `toString(SourcePort)`.
	
	Подробнее о создании SQL-запроса в конструкторе запроса см. ниже.
	
	Существуют следующие ограничения:
	
	• Псевдонимы `metric` и `value` в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по событиям, кроме таблиц.
	• Псевдонимы в виджетах с графиком типа **Таблица** могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"Псевдоним с пробелом"`, `` `Другой псевдоним` ``.
	• Не поддерживается использование SQL-запроса `ARRAY JOIN`.
	• При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать 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 слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

    Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

  - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

    Период рассчитывается относительно настоящего времени.

  - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

    Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

    В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени 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 LogAnalyzer хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме **now**), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

Границы периода включаются: например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 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**.

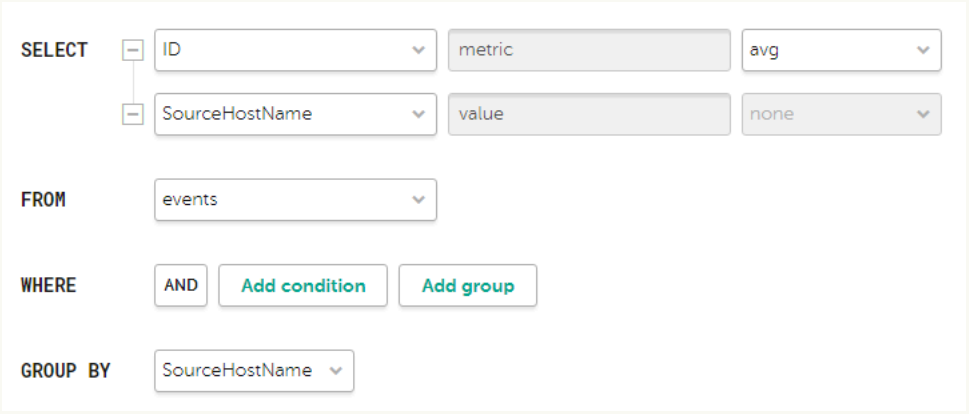
e. **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

- 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**.

Параметр	Описание
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
Название	Название виджета.
Описание	Описание виджета.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**. Параметр доступен для графиков типа **Столбчатая диаграмма**, **Счетчик**, **Линейная диаграмма**, **Календарная диаграмма**.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа **Столбчатая диаграмма**, **Календарная диаграмма** (с видом диаграммы **Столбчатая диаграмма**), **Таблица**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
Итоговые значения	Суммы значений.
Длительность отрезков периода	Длительность отрезков, на которые требуется делить период. Доступно для графика типа **Календарная диаграмма**.

Параметр	Описание
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

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.

Обращение в Службу технической поддержки

Если вам не удается найти решение своей проблемы в документации к программе, обратитесь в Службу технической поддержки "Лаборатории Касперского".

"Лаборатория Касперского" предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ).

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 LogAnalyzer можно обращаться из сторонних решений с помощью API. LogAnalyzer 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 LogAnalyzer>:<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 LogAnalyzer.
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 LogAnalyzer, 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 LogAnalyzer **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 LogAnalyzer для каждого пользователя можно настроить операции, которые можно выполнять от лица этого пользователя. Права можно настроить только для пользователей, созданных в LogAnalyzer.

Чтобы настроить доступные операции для пользователя:

1. Откройте раздел веб-интерфейса LogAnalyzer **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 LogAnalyzer ошибки имеют следующий формат:

```
type Error struct {
    Message    string      `json:"message"`
    Details    interface{} `json:"details"`
}
```

Операции REST API v3

В LogAnalyzer доступен ограниченный набор методов REST API по сравнению с KUMA.

Открыть справку по REST API

В таблице ниже приведен список методов REST API, доступных в базовой и коммерческой версии LogAnalyzer. Методы REST API, описанные в справке по REST API, но не указанные в таблице ниже, недоступны в LogAnalyzer.

Методы REST API, доступные в базовой и коммерческой версии LogAnalyzer

Метод REST API	Описание	Доступность в базовой версии LogAnalyzer	Доступность в коммерческой версии LogAnalyzer
Словари			
GET /dictionaries	Получение словаря	–	✓

Метод REST API	Описание	Доступность в базовой версии LogAnalyzer	Доступность в коммерческой версии LogAnalyzer
POST /dictionaries/add_row	Добавление или изменение строки с указанным ключом в словаре, который определяется указанным идентификатором словаря	—	✓
POST /dictionaries/delete_row	Удаление строки с указанным ключом в словаре, который определяется указанным идентификатором словаря	—	✓
POST /dictionaries/update	Обновление словаря в сервисах	—	✓
События			
POST /events	Поиск событий	✓	✓
GET /events/clusters	Просмотр информации о кластере	✓	✓
Папки			
GET /folders	Поиск папок	✓	✓
Отчеты			
GET /reports	Поиск отчетов	✓	✓
Ресурсы			
GET /resources	Поиск ресурсов	—	✓
POST /resources/export	Экспорт ресурсов	—	✓
POST /resources/import	Импорт ресурсов	—	✓
POST /resources/toc	Просмотр содержимого файла с ресурсами	—	✓
POST /resources/upload	Загрузка файла с ресурсами	—	✓
POST /resources/:kind/create	Создание ресурса указанного типа	—	✓
POST /resources/:kind/validate	Проверка содержимого ресурса	—	✓
GET /resources/:kind/:id	Получение ресурса с указанным типом и идентификатором	—	✓
PUT /resources/:kind/:id	Изменение ресурса с указанным типом и идентификатором	—	✓
GET /resources/:kind/:id/history	Получение всех версий ресурса по указанному типу и идентификатору	—	✓
GET /resources/:kind/:id/history/:changeNumber	Получение прошлой версии ресурса по указанному типу, идентификатору и номеру версии	—	✓
POST /resources/:kind/:id/history/:changeNumber	Восстановление прошлой версии ресурса по указанному типу, идентификатору и номеру версии	—	✓
Сервисы			
GET /services	Поиск сервисов	✓	✓
POST /services/create	Создание сервиса на основе ресурса, указанного в теле запроса	✓	✓
POST /services/:id/reload	Перезагрузка сервиса	✓	✓
POST /services/:id/restart	Перезапуск сервиса	✓	✓
Система			
GET /system/backup	Создание резервной копии Ядра LogAnalyzer	✓	✓
POST /system/restore	Восстановление Ядра LogAnalyzer из резервной копии	✓	✓
Задачи			

Метод REST API	Описание	Доступность в базовой версии LogAnalyzer	Доступность в коммерческой версии LogAnalyzer
POST /tasks/create	Создание задачи	✓	✓
Тенанты			
GET /tenants	Поиск тенантов	✓	✓
POST /tenants/create	Создание тенанта	✓	✓
Пользователи			
GET /users	Поиск пользователей	✓	✓
GET /users/id/:id	Поиск пользователя по идентификатору	✓	✓
GET /users/whoami	Просмотр информации о предъявителе токена	✓	✓

Приложения

В этом разделе представлены приложения к основному тексту документа.

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла LogAnalyzer /opt/kaspersky/kuma/kuma, с помощью которого можно вручную запустить или установить компоненты LogAnalyzer. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Параметры команд

Команды	Описание
`tools`	Запуск инструментов управления LogAnalyzer.
`collector`	Установка, запуск или удаление сервиса коллектора.
`core`	Установка, запуск или удаление сервиса Ядра.
`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 программы.

Флаги:

`-h`, `--h` используются для получения справочной информации о командах файла kuma. Например: `kuma <компонент> --help`.

Примеры:

- `kuma version` – получение информации о версии установщика LogAnalyzer.
- `kuma core -h` – получение справки по команде `core` установщика LogAnalyzer.
- `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 LogAnalyzer

Проверить целостность компонентов LogAnalyzer вы можете следующими способами:

- Вручную, запустив скрипт, приведенный ниже.
- По расписанию или автоматически при запуске приложения с записью результатов в системный журнал.

Проверка целостности вручную

Целостность компонентов LogAnalyzer 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/integrity/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 LogAnalyzer 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 LogAnalyzer вы хотите проверить:

   - `./check_all.sh` – компоненты Ядра LogAnalyzer и хранилища;
   - `./check_core.sh` – компонент Ядра LogAnalyzer;
   - `./check_collector.sh` – компонент коллектора LogAnalyzer;
   - `./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 LogAnalyzer 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 LogAnalyzer без указания имени файла>` – агент LogAnalyzer 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 LogAnalyzer.
  - Directories – при проверке целостности LogAnalyzer не используется.
  - Registries – при проверке целостности LogAnalyzer не используется.
  - Registry values – при проверке целостности LogAnalyzer не используется.
- Результат проверки целостности компонента:
  - SUCCEEDED – целостность подтверждена.
  - FAILED – целостность нарушена.

По расписанию или автоматически при запуске приложения

Так как LogAnalyzer – это распределенное, многокомпонентное решение и расположение компонентов на хостах определяется на этапе установки, настройка автоматической проверки целостности компонентов не может быть прописана в дистрибутиве решения и должна производиться на этапе развертывания.

Мы рекомендуем проверять целостность компонентов LogAnalyzer на этапе запуска приложения и по расписанию. Рекомендуемая периодичность проверки по расписанию – раз в сутки. Вы можете сделать это с помощью скриптов. Для получения скриптов обратитесь в Службу технической поддержки:

- manual_integrity_check.sh

  Скрипт проверяет целостность всех или выбранных вами компонентов. Проверку целостности по расписанию можно настроить с помощью сторонних приложений и утилит, например с помощью утилиты Cron. Вы также можете запускать этот скрипт для проверки целостности компонентов вручную.

- systemd_integrity_check.sh

  Используйте этот скрипт для самотестирования целостности компонентов приложения на этапе запуска. Чтобы добавить автоматическую проверку целостности, запустите этот скрипт на каждом хосте, на котором установлены компоненты LogAnalyzer. Скрипт следует запустить однократно. Целостность компонента будет проверяться при каждом запуске или перезапуске сервиса LogAnalyzer.

  Если после развертывания вы добавите новые сервисы LogAnalyzer (например, новый коллектор), запустите скрипт systemd_integrity_check.sh на хостах с новыми сервисами. В противном случае целостность новых компонентов на этапе запуска проверяться не будет.

  Если в результате проверки целостность компонента не подтвердится, компонент не будет запущен. LogAnalyzer продолжит попытки запустить сервис, предварительно проверив его целостность. Результаты проверки будут записываться в журнал системного аудита. В таком случае либо остановите сервис, либо устраните причину нарушения целостности.

Предварительные условия

Перед запуском скриптов вам нужно выполнить следующие действия:

- Перенести файлы скриптов в папку /opt/kaspersky/kuma/integrity/bin/.
- Назначить учетной записи kuma необходимые права для запуска скриптов. Для этого выполните следующие команды:

  ```
  chown kuma:kuma ./systemd_integrity_check.sh
  chmod +x ./systemd_integrity_check.sh
  chown kuma:kuma ./manual_integrity_check.sh
  chmod +x ./manual_integrity_check.sh
  ```

Запуск скриптов

Скрипт manual_integrity_check.sh

Для проверки целостности компонентов запустите скрипт на хосте, на котором установлены компоненты LogAnalyzer:

```
/opt/kaspersky/kuma/integrity/bin# ./manual_integrity_check.sh --core --collector --eventRouter --correlator --storage
```

Скрипт проверяет целостность тех компонентов, флаги для которых вы указали в командной строке. Если флаги не указаны, скрипт проверяет все компоненты.

Скрипт systemd_integrity_check.sh

Чтобы добавить автоматическую проверку целостности компонентов приложения на этапе запуска или перезапуска сервиса LogAnalyzer, выполните команду:

```
/opt/kaspersky/kuma/integrity/bin# ./systemd_integrity_check.sh
```

Оба скрипта заносят результаты проверки целостности компонентов в журнал системного аудита. Для просмотра журнала воспользуйтесь командой dmesg:

```
sudo dmesg
```

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события LogAnalyzer. 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.
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, 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.
BaseEvents	Вложенный список [Event]	-	Вложенная структура со списком базовых событий.

Code	Строка	-	В базовом событии это код возврата процесса, функции или операции из источника.
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.
ID	Строка	-	Уникальный идентификатор события типа UUID. Для базового события, генерируемого на коллекторе, идентификатор генерирует коллектор. 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: 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 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 LogAnalyzer

LogAnalyzer 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
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

Событие	Поле исходного события	Поле нормализованного события
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
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

Событие	Поле исходного события	Поле нормализованного события
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
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 учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты.

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.
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 LogAnalyzer

События аудита создаются при выполнении в LogAnalyzer определенных действий, связанных с безопасностью, и используются для обеспечения целостности системы.

Чтобы просмотреть события аудита, вам нужно перейти в раздел LogAnalyzer **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 LogAnalyzer 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`

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные ниже.

Название поля события	Значение поля
`Timestamp`	Время события.
`DeviceHostName`	Хост источника события. Для событий аудита это имя хоста, на котором установлена служба kuma-core, потому что она является источником событий.
`DeviceTimeZone`	Часовой пояс системного времени сервера, на котором установлено Ядро LogAnalyzer в формате `+-чч:мм`.
`Type`	Тип события аудита. `Audit` или `Base`.
`TenantID`	Идентификатор главного тенанта.
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`EndTime`	Время создания события.
`SpaceID`	`KUMA Audit`

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

Роль пользователя изменена

Название поля события	Значение поля
DeviceAction	user role 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 использовался для изменения данных.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных.

DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение роли.
DeviceCustomString1Label	new role
DeviceCustomString2	Значение роли до ее изменения.
DeviceCustomString2Label	old role

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 использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID 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 использовался для создания учетной записи.
SourceUserID	Идентификатор пользователя, который использовался для создания учетной записи.
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, для которого вносились изменения данных.
SourceUserID	Идентификатор пользователя, для которого вносились изменения данных.
DestinationUserPrivileges	Название роли. Доступные значения: general admin, admin, analyst, operator.
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 вносит изменения.
SourceUserID	Идентификатор пользователя, который вносит изменения.
DestinationUserName	Логин пользователя, для которого вносятся изменения.
DestinationUserID	Идентификатор пользователя, для которого вносятся изменения.
DestinationUserPrivileges	Название роли. Доступные значения: general admin, admin, analyst, operator.
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 вносит изменения.

SourceUserID	Идентификатор пользователя, который вносит изменения.
DeviceCustomString5	Обновленный набор полей, | используется в качестве разделителя.

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 использовался для изменения данных.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.

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 использовался для изменения параметров.
SourceUserID	Идентификатор пользователя, который использовался для изменения параметров.
DeviceCustomString5	Идентификатор набора пространств.
DeviceCustomString5Label	set ID
DeviceCustomString3	Название набора пространств.
DeviceCustomString3Label	space 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 использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID 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 использовался для удаления сервиса.
SourceUserID	Идентификатор пользователя, который использовался для удаления сервиса.
DeviceExternalID	ID 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 использовался для перезагрузки сервиса.
SourceUserID	Идентификатор пользователя, который использовался для перезагрузки сервиса.
DeviceExternalID	ID 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 использовался для перезапуска сервиса.
SourceUserID	Идентификатор пользователя, который использовался для перезапуска сервиса.
DeviceExternalID	ID 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	ID 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	ID 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	ID 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

Индекс партиции удален 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 использовался для удаления.
SourceUserID	Идентификатор пользователя, который использовался для удаления.
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

Раздел хранилища автоматически удален в связи с истечением срока действия

Название поля события	Значение поля
DeviceAction	applied retention policy by days.
EventOutcome	succeeded или failed
Name	Название хранилища | Тенант перемещаемого или удаляемого раздела | Название пространства, которому принадлежит раздел.
DeviceCustomDate1	Дата создания раздела.
DeviceCustomDate1Label	date of partition
SourceServiceName	scheduler
DeviceCustomString1	Идентификатор узла.
DeviceCustomString1Label	nodeID
Message	В случае перемещения: • Если EventOutcome = succeeded, отображается сообщение moved partition data to cold storage. • Если EventOutcome = failed, отображается сообщение об ошибке move partition data to cold storage failed: < описание ошибки >. В случае удаления: • Если EventOutcome = succeeded, отображается сообщение deleted partition data. • Если EventOutcome = failed, отображается сообщение об ошибке delete partition data failed: < описание ошибки >.
DeviceCustomNumber1	Размер раздела хранилища в байтах.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий в разделе хранилища.
DeviceCustomNumber2Label	events

Раздел хранилища автоматически удален или перемещен в связи с превышением объема хранилища

Для разделов хранилища в LogAnalyzer устанавливается условие для автоматического перемещения или удаления раздела диска при достижении или превышении указанного максимального объема такого раздела. Максимальный объем хранилища может быть определен одним из следующих способов:

- указывается процент от объема всего раздела диска, где установлено хранилище;
- определяется значение объема раздела диска в ГБ.

Если при проверке выполнения условия устанавливается, что объем хранилища равен или превышает установленный объем в процентах или ГБ, создается событие аудита и выполняется перемещение или удаление раздела хранилища.

Название поля события	Значение поля
DeviceAction	Если объем раздела хранилища определен в процентах от объема диска, то значение – `applied retention policy by percent`. Если объем раздела хранилища определен в ГБ, то значение – `applied retention policy by GB`.
EventOutcome	`succeeded` или `failed`
Name	Название хранилища | Тенант перемещаемого или удаляемого раздела | Название пространства, которому принадлежит раздел.
DeviceCustomDate1	Дата создания раздела.
DeviceCustomDate1Label	`date of partition`
SourceServiceName	`scheduler`
DeviceCustomString1	Идентификатор узла, который запустил очистку хранилища в связи с достижением максимального размера занятого пространства.
DeviceCustomString1Label	`retention policy trigger node`
Message	В случае перемещения: • Если `EventOutcome = succeeded`, отображается сообщение `moved partition data to cold storage`. • Если `EventOutcome = failed`, отображается сообщение об ошибке `move partition data to cold storage failed: < описание ошибки >`. В случае удаления: • Если `EventOutcome = succeeded`, отображается сообщение `deleted partition data`. • Если `EventOutcome = failed`, отображается сообщение об ошибке `delete partition data failed: < описание ошибки >`.
DeviceCustomNumber1	Размер раздела хранилища в байтах.
DeviceCustomNumber1Label	`size`
DeviceCustomNumber2	Количество событий в разделе хранилища.
DeviceCustomNumber2Label	`events`

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

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.
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

Изменена политика хранения данных после изменения дисков или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	storage policy modified
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 изменения данных тенанта.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных тенанта.

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.

Отправка тестовых событий в LogAnalyzer

В LogAnalyzer предусмотрена отправка тестовых событий в систему. Используйте опцию отправки тестовых событий в LogAnalyzer, 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 LogAnalyzer:

   a. В веб-интерфейсе LogAnalyzer 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 LogAnalyzer **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 LogAnalyzer, 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 LogAnalyzer. Вы можете проверить поступление тестовых событий, выполнив поиск связанных событий в веб-интерфейсе LogAnalyzer.

Формат времени

LogAnalyzer 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".
- "13842163671112223333".

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 LogAnalyzer 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 LogAnalyzer 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.
[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.

Название	Тип ресурса	Описание
[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.

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 LogAnalyzer.

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 LogAnalyzer **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 LogAnalyzer 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 LogAnalyzer

Служба LogAnalyzer, которая предоставляет пользовательский интерфейс для настройки и отслеживания операций LogAnalyzer.

Кластер

Группа серверов, на которых установлена программа LogAnalyzer и которые были сгруппированы для централизованного управления с помощью веб-интерфейса программы.

Коллектор

Компонент LogAnalyzer, который получает сообщения из источников событий, обрабатывает их и передает в хранилище и/или сторонние сервисы для выявления подозрений на инциденты ИБ.

Коннектор

Компонент LogAnalyzer, обеспечивающий транспорт для приема данных из внешних систем.

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 LogAnalyzer. 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 LogAnalyzer, который используется, чтобы сформировать набор данных по критериям фильтра, заданным пользователем.

Панель мониторинга

Компонент системы LogAnalyzer, выполняющий визуализацию данных.

Парсинг

Процесс организации данных и приведения поступающих событий в формат LogAnalyzer.

Роль

Набор прав доступа, установленных для предоставления пользователю веб-интерфейса LogAnalyzer 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 LogAnalyzer.

Фильтр

Набор условий, которые программа 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 и Apache Cassandra 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 – товарный знак, права на который принадлежат компании SolarWinds Worldwide, LLC или аффилированным лицам компании, зарегистрирован в Бюро по патентам и товарным знакам США, а также может быть зарегистрирован или находиться в процессе регистрации в других странах.

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, 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 является товарным знаком 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.

Microsoft, Active Directory, 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 – 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 – товарный знак компании YANDEX LLC.

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.

Список ограничений

LogAnalyzer имеет ряд ограничений, не критичных для работы приложения:

- После обновления LogAnalyzer 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.